ESCUELA POLITÉCNICA DEL EJÉRCITO

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

DESARROLLO DE UN MANUAL DE AUDITORÍA INFORMÁTICA APLICADO A COOPERATIVAS DE AHORRO Y CRÉDITO

Tesis de Grado

Autor: Ing. Carlos Alberto Sarango Ontaneda

Sangolquí, 2013

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por el Señor Ingeniero CARLOS ALBERTO SARANGO ONTANEDA como requerimiento parcial a la obtención del Título de MAGISTER EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS.

Sangolquí, 18 de marzo de 2013.

Ing. PAULO BERMEO MANCERO, MBA.

DECLARACIÓN DE RESPONSABILIDAD

Declaro que:

La tesis de grado titulada: Desarrollo de un Manual de Auditoría Informática Aplicado a Cooperativas de Ahorro y Crédito, ha sido desarrollada en base a una investigación, respetando derechos intelectuales de terceros, cuyas fuentes son citadas e incorporadas en la bibliografía, consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico de esta tesis.

Sangolquí, 18 de marzo de 2013.

Ing. CARLOS ALBERTO SARANGO ONTANEDA

AUTORIZACIÓN

Yo, Carlos Alberto Sarango Ontaneda autorizo a la Escuela Politécnica del Ejército, la publicación en la biblioteca virtual de la institución, de la tesis de grado titulada: Desarrollo de un Manual de Auditoría Informática Aplicado a Cooperativas de Ahorro y Crédito, cuyo contenido, idea y criterios son de mi responsabilidad y autoría.

Sangolquí, 18 de marzo de 2013.

Ing. CARLOS ALBERTO SARANGO ONTANEDA

AGRADECIMIENTO

A Dios, por darme vida, salud y fuerza para conseguir lo anhelado.

A mi esposa, a mi hija, a mi madre, a mi familia y amigos que confiaron en mí y me brindaron su apoyo sobre todo en los momentos difíciles.

Al Ing. Paulo Bermeo MBA, cuya dirección y asesoría fueron fundamentales en el desarrollo del presente proyecto.

A mis compañeros y colegas de quienes aprendo día con día.

Mi más sincero agradecimiento a todas las personas que de una u otra manera colaboraron en el desarrollo del presente proyecto de titulación.

Muchas gracias a todos.

Carlos Alberto Sarango O.

DEDICATORIA

A Sonia, mi compañera de vida y a María José, mi espléndida hija, que me inspiran a convertir los sueños en realidad.

ÍNDICE DE CONTENIDOS

Certificación……..……..……..……..……..I

Declaración de Responsabilidad…….……..……..……..……..II

Autorización…….....……..……..……..……..……..……..III

Agradecimiento……..……..……..……..……..……..……..IV

Dedicatoria..……..……..……..……..……..……..……..V

Índice de Contenidos..……..……..……..……..……..……..VI

Índice de Tablas……..……..……..……..……..……..……..XI

Índice de Figuras.…...……..……..……..……..……..……..XII

Introducción……..……..……..……..……..……..……..XIII

Resumen…..……..……..……..……..……..……..……XIV

Abstract..……..……..……..……..……..……..……..XVI

CAPÍTULO 1.....1

INTRODUCCIÓN.....1

1.1 ANTECEDENTES 1

1.2 JUSTIFICACIÓN E IMPORTANCIA.....3

1.3 PLANTEAMIENTO DEL PROBLEMA 4

1.4 FORMULACIÓN DEL PROBLEMA 5

1.5 OBJETIVO GENERAL.....6

1.6 OBJETIVOS ESPECÍFICOS 6

CAPÍTULO 2.....8

EL SECTOR COOPERATIVO FINANCIERO.....8

2.1 El Cooperativismo 8
2.1.1 Historia del Cooperativismo 8
2.1.2 El Sistema Cooperativo en el Ecuador 9
2.1.2.1 Orígenes y primeras manifestaciones 10
2.1.2.2 El Sistema Cooperativo de Ahorro y Crédito 12
2.1.2.3 Las Cooperativas de Ahorro y Crédito en lo Económico y Financiero . 14
2.2 Desarrollo del Marco Legal y Regulatorio de las Instituciones Financieras 16
2.3 Marco Regulatorio del Sector Cooperativista de Ahorro y Crédito .. 20
2.3.1 La Ley de Economía Popular y Solidaria 22
2.3.2 Cooperativas Reguladas por la Superintendencia de Bancos y Seguros 25
2.3.3 Tamaño de las Cooperativas Controladas por la SBS 28
2.4 El Control en las Cooperativas de Ahorro y Crédito Supervisadas por la SBS 30
2.4.1 El Control Interno 31
2.4.2 La Administración de Riesgos 33
2.4.3 La Auditoría Interna 36

CAPÍTULO 3 40

MARCO TEÓRICO 40

3.1 Introducción 40
3.2 El Control Interno y su Evolución 40
3.2.1 Coso I 42
3.2.2 Coso Erm 43
3.2.2.1 Componentes de Coso ERM 45
3.2.3 Cobit4.1 47
3.2.3.1 Estructura de Cobit 4.1 49
3.2.3.1.1 ¿Qué es un proceso? 54
3.2.3.1.2 Los Recursos de TI 55
3.2.3.1.3 Los Controles 56
3.2.3.1.4 Aceptabilidad General de COBIT 57

3.2.3.2 Cobit Quickstart 60
3.2.3.2.1 Cobit Quickstart y las Pymes 61
3.2.3.2.2 Estructura de Cobit Quickstart 64
3.2.3.2.3 Usuarios de Cobit Quickstart 66
3.2.3.2.4 ¿Cómo saber si Quickstart es adecuado para mi organización? 66
3.2.4 LOS CONTROLES 70
3.2.4.1 Controles Generales 70
3.2.4.2 Controles de Sistemas de Información 72
3.3 LA GESTIÓN DE RIESGO DE TI 73
3.3.1 MAGERIT VERSIÓN 2 76
3.3.1.1 Objetivos de Magerit 76
3.3.1.2 Análisis y Gestión de Riesgos 77
3.3.1.3 Proceso de Análisis de Riesgos 78
3.4 EL PROCESO DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN 80
3.4.1 ANTECEDENTES 80
3.4.2 LA FUNCIÓN DE AUDITORÍA INFORMÁTICA 81
3.4.2.1 Definiciones 81
3.4.2.1.1 Auditoría 81
3.4.2.1.2 Clasificación de las Auditorías 81
3.4.2.1.3 Auditoría Informática 83
3.4.2.2 Planeación de la Auditoría 85
3.4.2.2.1 Planeación Anual 85
3.4.2.2.2 Planeación de Auditorías Individuales 86
3.4.2.3 Marco Normativo para la Auditoría Informática (Isaca) 87
3.4.2.3.1 Código de Ética Profesional de Isaca 88
3.4.2.3.2 Normas de Auditoría Informática 90
3.4.2.3.3 Directrices de Auditoría Informática 94
3.4.3 ESTATUTO DE AUDITORÍA 96
3.4.4 AUDITORÍA BASADA EN RIESGOS 97

CAPÍTULO 4 100

MODELAMIENTO DEL MANUAL DE AUDITORÍA INFORMÁTICA 100

4.1 EL PROBLEMA 100
4.1.1 ¿POR QUÉ SE REQUIERE UNA AUDITORÍA DE SISTEMAS? 100
4.2 PROCESO DE AUDITORÍA PROPUESTO 102

4.2.1 PROCESO PARA LA PLANEACIÓN ANUAL DE AUDITORÍA 102
4.2.1.1 Comprender Objetivos y Procesos 104
4.2.1.2 Identificar Objetivos y Riesgos 104
4.2.1.3 Evaluación de Riesgos 105
4.2.1.4 Análisis de Proceso y Riesgo 105
4.2.1.5 Definición del Plan 105
4.2.2 PROCESO PARA UNA ASIGNACIÓN INDIVIDUAL DE AUDITORÍA 106
4.2.2.1 Recopilar Información y Planear 108
4.2.2.2 Lograr Entendimiento del Control Interno 108
4.2.2.3 Efectuar Pruebas de Cumplimiento 109
4.2.2.4 Efectuar Pruebas Sustantivas 110
4.2.2.5 Concluir la Auditoría 110
4.3 MANUAL DE AUDITORÍA INFORMÁTICA 110
4.3.1 ESTRUCTURA 110

CAPÍTULO 5 112

APLICACIÓN DEL MANUAL DE AUDITORÍA INFORMÁTICA 112

5.1 EL CASO DE LA COOPERATIVA INTERNACIONAL 112
5.1.1 LA HISTORIA 112
5.1.2 ESTRUCTURA DE LA COOPERATIVA 114
5.1.3 APLICACIONES E INFRAESTRUCTURA 115
5.2 APLICACIÓN DEL MANUAL 117
5.2.1 DEFINIR EL PLAN ANUAL DE AUDITORÍA 117
5.2.1.1 Comprender los Objetivos del Negocio 118
5.2.1.2 Identificar Objetivos y Riesgos de TI 119
5.2.1.3 Evaluación de Riesgos 121
5.2.1.4 Análisis de Proceso y Riesgo 128
5.2.1.5 Definición del Plan 133
5.2.2 REVISIÓN INDIVIDUAL DE AUDITORÍA 135
5.2.2.1 Recopilar Información y Planear 136
5.2.2.2 Lograr Entendimiento del Control Interno 140

5.2.2.3 Efectuar Pruebas de Cumplimiento 143
5.2.2.4 Efectuar Pruebas Sustantivas 145
5.2.2.5 Concluir la Auditoría 146

CAPÍTULO 6 148

CONCLUSIONES Y RECOMENDACIONES 148

6.1 CONCLUSIONES 148
6.2 RECOMENDACIONES 151

BIBLIOGRAFÍA 156

ABREVIATURAS Y ACRÓNIMOS 160

ANEXOS 161

ÍNDICE DE TABLAS

Pág.

Tabla 1.1 Cooperativas de Ahorro y Crédito Supervisadas por la SBS 27

Tabla 1.2 Tamaño de las COACs Supervisadas por la SBS 29

Tabla 3.1 Lista de Procesos Cobit 4.1 (Cobit 4.1, 2007).....53

Tabla 3.2 Comparación de Cobit Quickstart con Cobit 4.1 61

Tabla 5.1 Niveles para valoración de impacto, probabilidad y control 124

Tabla 5.2 Escala para definir el nivel de riesgo 124

Tabla 5.3. Definición de Riesgo Inherente.....125

Tabla 5.4 Valoración de Riesgo Residual.....127

Tabla 5.5 Riesgos Seleccionados.....128

Tabla 5.6 Matriz de Proceso/Riesgo.....132

Tabla 5.7 Ciclos de Revisión de Procesos.....133

Tabla 5.8 Ciclos Definidos de Revisión de los Procesos de TI 134

Tabla 5.9 Resumen de Valoración de Activos 137

Tabla 5.10 Calificación de Riesgo Inherente 139

Tabla 5.11 Nivel de riesgo de control del proceso 141

Tabla 5.12 Porcentaje de Riesgo por Nivel.....142

Tabla 5.13 Cálculo del riesgo de detección 142

ÍNDICE DE FIGURAS

Pág.

Figura 3.1 Componentes de Control Interno 43
Figura 3.2 Principio básico de Cobit (Cobit 4.1, 2007).....51
Figura 3.3 Dominios Interrelacionados de Cobit (Cobit 4.1, 2007).....52
Figura 3.4 Estructura conceptual del proceso.....54
Figura 3.5 Manteniéndose en la zona azul (Cobit Quickstart, 2007).....67
Figura 3.6 Herramienta de Calor (Cobit Quickstart, 2007).....70
Figura 3.7 Análisis de Riesgos (Magerit, 2006) 80
Figura 3.8 Enfoque de Auditoría Basado en Riesgos (ISACA, 2009) 99
Figura. 4.1 Proceso de Planeación Anual de Auditoría Informática.....103
Figura 4.2 Proceso de Auditoría Informática con Enfoque a Riesgos.....107
Figura 5.1 Matriz de Amenazas y Objetivos TI 122
Figura 5.2 Dimensiones del Riesgo 123

INTRODUCCIÓN

El presente documento corresponde a una investigación realizada por el autor, con el fin de aplicar y profundizar en los contenidos académicos recibidos en el programa de Maestría en Evaluación y Auditoría de Sistemas Tecnológicos, ofrecido por la Escuela Politécnica del Ejército.

La tesis se desarrolla en un escenario identificado con la realidad nacional, como es el sector de Cooperativas de Ahorro y Crédito. Se busca atender desde la perspectiva de auditoría interna, las necesidades de evaluación de la gestión tecnológica de dichas instituciones.

El objetivo primordial de este proyecto es diseñar y documentar las actividades concernientes a los procesos de auditoría necesarios para realizar una auditoría informática en una Cooperativa de Ahorro y Crédito.

Dicha tarea se desarrolla considerando las perspectivas de control, análisis de riesgos y mejores prácticas de la industria, se adaptan estos conceptos y se registran los resultados en el documento final que corresponde al Manual de Auditoría Informática.

RESUMEN

La auditoría informática es una función (en ocasiones un servicio) que apoya al trabajo de las unidades de auditoría interna de las Cooperativas de Ahorro y Crédito. Sin embargo, el trabajo a realizarse exige que los profesionales en auditoría informática cumplan con ciertas normas y requerimientos tanto legales como profesionales. El uso de marcos de buenas prácticas, análisis de riesgos y la observación de las normas de auditoría son fundamentales para el desarrollo de las evaluaciones de auditoría informática. Es por tanto que el presente proyecto busca integrar dichos requerimientos en una propuesta enfocada a evaluar los procesos tecnológicos de las Cooperativas de Ahorro y Crédito. La mencionada propuesta ha sido plasmada en el presente estudio, mismo que consta de seis capítulos que se describen a continuación.

En el primer capítulo se describe las consideraciones básicas del problema a tratar, se justifica la importancia del proyecto se definen los objetivos tanto generales como específicos de la investigación.

El segundo capítulo muestra una panorámica del sistema cooperativo de ahorro y crédito, se describe su evolución en el tiempo y se analiza el marco legal en el cual se desarrolla. Este capítulo finaliza destacando los requerimientos legales que dan lugar al trabajo de auditoría informática en las COACs.

El tercer capítulo desarrolla el marco teórico, estableciendo la estructura conceptual de la investigación. Aquí se tratan las normas y marcos de buenas prácticas internacionales orientados hacia áreas como: auditoría de sistemas, gestión de riesgos, gobierno de tecnología de información y control interno. La investigación realizada brinda el soporte teórico a la propuesta a desarrollarse.

En el capítulo cuatro se desarrolla el manual de auditoría informática, se inicia analizando las interrogantes del problema, para luego establecer los dos macro procesos que serán tratados en el manual. Se describe las actividades de cada proceso, sus entregables y finalmente se diseña la estructura del manual de auditoría informática para COACs, el documento del manual se encuentra como adjunto a este capítulo.

El capítulo cinco muestra la aplicación del manual de auditoría informática desarrollado, a título de ejemplo se analiza el caso de una Cooperativa de Ahorro y Crédito, se siguen las instrucciones del manual para realizar la planificación anual de auditoría informática así como para auditar un proceso tecnológico específico.

Finalmente en el capítulo seis se detallan las conclusiones y recomendaciones generadas por el desarrollo del presente proyecto.

ABSTRACT

Informatic audit is a function, and occasionally a service, that supports the operations of the internal audit units of Cooperativas de Ahorro y Crédito (Cooperatives of Savings and Credit). Moreover, the tasks in hand demand that professionals working in informatics audit meet certain norms and requirements – both legal and professional. The use of best practice frameworks, risk analysis and compliance with audit norms are essential for the development of evaluations of informatic audit. These are the reasons why the current project seeks to integrate all these requirements in a proposal which will focus on evaluating the technological processes of Cooperativas de Ahorro y Crédito. The aforementioned proposal has been converged in the current study, which is composed of six chapters. The following is the description of each.

In the first chapter the basic considerations of the problems to deal with are described; the project's importance is justified; hypotheses are introduced; and the objectives of the investigation– both overall as well as specific – are defined.

The second chapter reveals a panoramic view of the cooperative system of savings and credit. In addition, it includes a description of its evolution and an analysis of the legal framework in which it evolves. The end of the chapter stresses the legal requirements which take place in informatic audits of the Cooperatives of Savings and Credit.

The third chapter develops the theoretical framework, while establishing the conceptual structures of the research. The chapter includes norms and best practice frameworks at the international level. These are focused in areas such as: systems audit, risk management, information technology government, and internal controls. The research performed provides the theoretical support to the proposal.

In the fourth chapter includes the manual of informatic audit. It begins with an analysis of the problem's main issues to be resolved, then it establishes the two macro processes encompassed in the manual. The activities for each process are described, as well as their deliverables. Finally, it provides the manual's structural design for the Cooperatives of Savings and Credit. The actual manual is included as an attached document to the chapter.

Chapter five describes the application of the generated manual for informatic audits. As an example, the Cooperative of Savings and Credit's case is analyzed. The instructions of the manual are followed to realize the annual planning of the informatics audit, as well as to perform an audit of the specific technological process.

Lastly, in chapter six details the conclusions and recommendations, generated throughout the project.

CAPÍTULO 1

INTRODUCCIÓN

1.1 Antecedentes

El 21 de enero de 2010 la Junta Bancaria presidida por la Ing. Gloria Sabando, emite mediante resolución las modificaciones a la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros de la Junta Bancaria. Dichas modificaciones corresponden al capítulo II “Normas para la calificación de los auditores internos de las entidades sujetas al control de la Superintendencia de Bancos y Seguros”, del título XXI “De las calificaciones otorgadas por la Superintendencia de Bancos y Seguros”, e incluyen la siguiente reforma: “Toda unidad de auditoría interna debe contar con un servicio de auditoría de sistemas de información, que colabore en el logro de sus funciones y objetivos. Este servicio debe contar con personal competente y experiencia específica en auditoría de sistemas, acorde con la complejidad y tamaño de las operaciones que realiza la institución del sistema financiero.”

Desde entonces la actividad de auditoría informática que se venía dando de forma opcional por parte de las instituciones financieras paso a ser un requerimiento obligatorio para todo el sector financiero ecuatoriano controlado por la Superintendencia de Bancos y Seguros.

La creciente dependencia tecnológica generada por el sector de servicios financieros, motivada principalmente por el aumento en la disponibilidad de nuevas y mayores redes de información, las altas inversiones

en infraestructura tecnológica y la implementación de esquemas de supervisión gubernamental más estrictos y detallados; han derivado en la necesidad de aplicar estructuras de auto control que permitan la entrega segura y sostenible de los servicios financieros. Como premisa, el establecimiento de dichos esquemas debe considerar la participación de entes independientes y competentes que evalúen y asesoren en el mejoramiento de los marcos de control empresariales.

Es en este escenario donde la función de auditoría tiene su papel principal, pues su trabajo se enfoca al desarrollo de evaluaciones que permitan asegurar el manejo de la información de negocio tanto operativa como estratégica. De esta forma, dicha función contribuye a la minimización de riesgos tales como: fraude interno y externo y el manejo poco eficiente de los recursos con la consabida afectación a los intereses de clientes y accionistas. Es importante señalar que la función de auditoría interna cuenta con varios equipos de trabajo cuyo enfoque obedece a los diferentes tipos de evaluación posibles (operativa, financiera, de procesos, metodológica, entre otras). La auditoría de tecnología de información (TI), de sistemas o simplemente auditoría informática constituye una pieza fundamental dentro del esquema de control interno y gestión de riesgo operativo de las entidades financieras.

Dentro del sector financiero regulado por la Superintendencia de Bancos y Seguros se encuentra el segmento de Cooperativas de Ahorro y Crédito, el mismo que agrupa a aquellas entidades que se encuentran bajo los principios de libre asociación, colaboración y solidaridad.

Si bien las Cooperativas de Ahorro y Crédito cuentan con un portafolio menor de servicios financieros con respecto al sector bancario, es importante señalar que gran parte de su operatividad y toma de decisiones se apoya en la gestión tecnológica, la cual le permite cumplir con los requerimientos del negocio y lograr una ventaja competitiva en el sector.

En base al escenario descrito, se identificó la necesidad de desarrollar un aporte enfocado al trabajo de auditoría informática ejecutado por las unidades de auditoría interna de las Cooperativas de Ahorro y Crédito. El objetivo principal del presente proyecto se traduce en el desarrollo de un documento (manual de auditoría) que sirva de guía para el desarrollo del proceso de Auditoria de Sistemas de Información en este segmento del sector financiero nacional.

1.2 Justificación e Importancia

El proyecto se justifica por las siguientes razones:

1. Por la necesidad de las Cooperativas de Ahorro y Crédito de contar con una evaluación integral de su gestión tecnológica.
2. Por la ausencia de un documento práctico que apoye el trabajo de evaluación tecnológica en entidades del sector de Cooperativas de Ahorro y Crédito.
3. Para apoyar el cumplimiento de la normativa legal emitida por la Superintendencia de Bancos y Seguros en lo relacionado a la gestión tecnológica de las instituciones del sector financiero Cooperativista.

4. Por la necesidad de enfocar las revisiones de auditoría interna hacia los procesos tecnológicos que generan mayor riesgo para la institución financiera.
5. Para procurar que las evaluaciones de auditoría informática soporten su trabajo en el marco de buenas prácticas de control Cobit 4.1.
6. Para realizar la evaluación de cada proceso tecnológico considerando su nivel de riesgo, lo que permite a su vez la definición de las pruebas específicas para cada control.
7. Para desarrollar una propuesta que integre los conceptos de Magerit versión 2.0 (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) y Cobit versión 4.1 (Control Objectives for Information and Related Technology), aplicables al trabajo de auditoría informática.

1.3 Planteamiento del Problema

La Codificación de Resoluciones de la SBS requiere que todas las unidades de auditoría interna de las instituciones financieras cuenten con un servicio de auditoría de sistemas, que colabore en el logro de los objetivos de dichas unidades. De igual forma el mencionado ente de control, mediante la normativa para la administración del riesgo operativo, definió varias actividades de control sobre el ambiente tecnológico, las cuáles deben ser implementadas por las instituciones financieras y cuyo cumplimiento requiere ser evaluado por el personal de auditoría informática de la institución. Este trabajo de revisión debe ser desarrollado por personal competente y con experiencia en auditoría

de sistemas y observando los requerimientos legales así como las normas y directrices especificadas para la profesión. La necesidad actual (tanto normativa como organizacional) enfatiza en el desarrollo de la auditoría basada en riesgos, de esta forma se promueve la evaluación y control de aquellos procesos y áreas que por su exposición al riesgo podrían generar mayores pérdidas a la entidad, sus socios y clientes. Por lo expuesto, es necesario para el personal de auditoría informática interna de las instituciones financieras (entre ellas las Cooperativas de Ahorro y Crédito), el contar con un conjunto de procedimientos específicos que lo guíen en la revisión de los procesos de tecnología, considerando la evaluación de riesgos, los objetivos de control y las normas de la profesión detalladas en documentos de estándares y buenas prácticas internacionales.

1.4 Formulación del Problema

La formulación del problema corresponde a dar respuesta a las siguientes preguntas derivadas de la realización de las actividades de auditoría informática enfocadas a Cooperativas de Ahorro y Crédito:

1. ¿El trabajo de auditoría informática considera marcos de buenas prácticas de control y análisis de riesgos enfocados a tecnología de la información?
2. ¿De qué forma seleccionar los procesos de TI a ser evaluados durante el año?
3. ¿Cómo se puede definir los controles a revisar para cada auditoría individual?

4. ¿Cómo se asegura que la auditoría de sistemas enfoca sus recursos hacia lo que es importante para la Cooperativa?

1.5 Objetivo General

Proponer un documento que sirva de referencia para auditar los principales procesos de tecnología de las Cooperativas de Ahorro y Crédito.

1.6 Objetivos Específicos

1. Analizar el sector de Cooperativas de Ahorro y Crédito, su historia y la normativa legal aplicable en el ámbito tecnológico (infraestructura y servicios)
2. Identificar el papel de la auditoría de tecnología de información como parte de las unidades de auditoría interna de las Cooperativas de Ahorro y Crédito.
3. Conocer y analizar los marcos de buenas prácticas de control interno y la metodología para análisis de riesgo tecnológico.
4. Investigar y analizar los conceptos, procesos y normativa referente al desarrollo del trabajo de auditoría informática.
5. Definir una propuesta que permita contar con un proceso de auditoría informática que considere la metodología para análisis y gestión de riesgos de los sistemas de información, Magerit versión 2 y los objetivos de control para la información y tecnología relacionada, Cobit 4.1.

6. Desarrollar un manual con las actividades, tareas y entregables requeridos para planificar y ejecutar la auditoría informática interna en Cooperativas de Ahorro y Crédito.
7. Desarrollar un ejemplo de la aplicación del manual de auditoría informática que permita guiar al lector en la aplicación del mencionado documento.
8. Generar las conclusiones y recomendaciones del proyecto.

CAPÍTULO 2

EL SECTOR COOPERATIVO FINANCIERO

2.1 El Cooperativismo

2.1.1 Historia del Cooperativismo

"El cooperativismo, a lo largo de su historia ha sido considerado y definido de múltiples formas: como doctrina política, modo de producción, sin embargo, actualmente se puede afirmar que el cooperativismo es un plan económico que forma parte importante de la vida de muchos países, y su desarrollo y difusión indica que podría llegar a modificar hasta la estructura política de las sociedades que las han implantado."[1]

Una de las características importantes de la teoría cooperativista es su sencillez, pues surge como resultado de la aplicación en gran medida del sentido común.

El movimiento cooperativo moderno mundial da inicio en el pueblo de Rochdale condado de Lancashire, Inglaterra. Fue en 1844 un grupo de 28 trabajadores de la industria textil, que vivían en este pueblo, trataron de controlar su destino económico formando una cooperativa llamada la Rochdale Equitable Pioneers Society (la Sociedad Equitativa de Pioneros de Rochdale).

En tal época la industria textil se encontraba en su apogeo y proporcionaba una gran actividad en las más importantes manufacturas de

[1]GESTIOPOLIS.COM - Ing.Com. M. Patricio Barzallo Mendieta, "Fundamentos Históricos Y Teóricos Del Sistema Cooperativo De Ahorro Y Crédito", agosto - 2002

Rochdale. Frente al desamparo de la clase trabajadora algunos tejedores recordaron las ideas de Robert Owen considerado el padre del cooperativismo.

Así, las cooperativas más antiguas son las de consumo, y su objetivo central es suministrar a los miembros de la misma, a precios módicos, los artículos que requieren para la satisfacción de sus necesidades. Pero es necesario indicar que el movimiento cooperativo no se limita a este ámbito, ya que también se han desarrollado diferentes clases de cooperativas de acuerdo a las necesidades del hombre.

La corriente religiosa de la Iglesia Católica tuvo su importancia en el desarrollo del sistema cooperativo a partir de varias encíclicas que buscaron mecanismos cooperativos para solucionar los problemas que afectaban a grandes capas de la población. Esta acción fue importante en los países de América Central y los de la Región Andina.

La corriente estatal de Latinoamérica tuvo inicio con medidas legislativas y de impacto muy significativas, que creaban un marco legal para el funcionamiento de las cooperativas. A partir de los años de 1950 y 1960 se brindó a través del Programa Alianza para el Progreso, un fuerte impulso al cooperativismo como inductor de progreso económico y social permitiendo además, que los Estados instituyeran oficinas especiales para la promoción, desarrollo y registro de cooperativas, canalizando así muchos de sus recursos y prestaciones hacia el cooperativismo.

2.1.2 El Sistema Cooperativo en el Ecuador

La legislación Cooperativa data de 1937, pero fue en la década del cincuenta al sesenta que cobró verdadera presencia en el ámbito nacional

cuando se da la creación de la mayor parte de las organizaciones Cooperativas, en esto intervinieron directa o indirectamente agentes ajenos a los sectores involucrados, es decir, instituciones públicas, privadas y promotores; entre estos últimos se puede señalar a religiosos, voluntarios extranjeros y algunos profesionales, a título personal o encargados por alguna organización de carácter político o social.[2]

Cabe citar también la acción desarrollada por los gremios, sindicatos de trabajadores, organizaciones clasistas y personal del movimiento cooperativo sobre todo norteamericano.

Esos antecedentes constituyeron indudablemente un elemento propicio para el afianzamiento en el país de las organizaciones empresariales de tipo cooperativo, cuyo cometido está reconocido y amparado por el Estado; pues, según lo establecido en la Ley respectiva, se las define como: ".... sociedades de derecho privado, formadas por personas naturales o jurídicas que, sin perseguir finalidades de lucro, tienen por objeto planificar o realizar actividades o trabajos de beneficio social o colectivo, a través de una empresa manejada en común y formada con la aportación económica, intelectual y moral de sus miembros"[3] .

2.1.2.1 Orígenes y primeras manifestaciones

En los orígenes y consolidación del movimiento cooperativo ecuatoriano se pueden distinguir por lo menos tres etapas fundamentales:

[2] NETICOOP - Giuseppina Da Ros, www.neticoop.org.uy/article173.html, febrero de 2004
[3] Congreso Nacional, “Ley de Cooperativas”, Art.1, Ecuador, 2001

- La primera se inicia aproximadamente en la última década del siglo XIX, cuando se crean -especialmente en Quito y Guayaquil- una serie de organizaciones artesanales y de ayuda mutua.
- La segunda empieza a partir de 1937, año en el cual se dicta la primera Ley de Cooperativas con el propósito de dar mayor alcance organizativo a los movimientos campesinos, modernizando su estructura productiva y administrativa, mediante la utilización del modelo cooperativista.
- la tercera etapa comienza a mediados de los años sesenta con la expedición de la Ley de Reforma Agraria (en 1964) y de la nueva Ley de Cooperativas (en 1966).

Actualmente, predominan las cooperativas de servicios y las de consumo, pero cabe destacar que las organizaciones que han sabido desarrollarse por iniciativa propia son las Cooperativas de Ahorro y Crédito, fortalecidas principalmente por la crisis bancaria del año 1999 que les permitió captar clientes de la banca cerrada.

En términos de membrecía, y comparando con los datos de mediados de la década de los ochenta, resulta que las cooperativas de ahorro y crédito ocupan actualmente el primer lugar con el 75.7% (en 1985 eran las últimas y aportaban con el 15.8%), seguidas de las de consumo (14.6%), de servicios (8.1%) y producción (1.6%). (Giuseppina Da Ros, 2004)

En síntesis, el sector cooperativista de mayor desarrollo y peso relativo en la economía nacional es indudablemente el de ahorro y crédito

2.1.2.2 El Sistema Cooperativo de Ahorro y Crédito

Es Friedrich Wilhelm Raiffeeisen (1818 – 1888), quien deja un legado a la humanidad con una rica experiencia en cooperativismo de ahorro y crédito. Raiffeeisen impulsó al sistema Cooperativo de Ahorro y Crédito, basado en los principios de auto ayuda, auto responsabilidad y auto administración, en su tiempo fundó varias cooperativas en su natal Alemania, y aquellos principios e ideas aún continúan vigentes en más de 100 países del mundo, con alrededor de 300 millones de socios, en más de 700.000 cooperativas.

En el Ecuador, la primera caja de ahorro que se fundó fue en la ciudad de Guayaquil, por obra de la Sociedad de Artesanos Amantes del Progreso, organización gremial constituida en 1879. Otras organizaciones mutualistas se constituyeron en años posteriores por obra de varios gremios.

Esporádicas manifestaciones del cooperativismo de crédito se registraron en los años veinte y cuarenta.

> Aunque en la década de los cincuenta dicho sector empieza a consolidarse (en 1955 se registraban 51 cooperativas de crédito, CONADE, 1983: IV), es solamente a partir de 1960 y bajo el auspicio de las agencias privadas norteamericanas CUNA y CLUSA que se observará un mayor crecimiento de este tipo de organizaciones. Dichas agencias contribuyeron a erigir los pilares fundamentales sobre los cuales reposa la actual estructura del cooperativismo de crédito

ecuatoriano, y, sobre todo, del de ahorro y crédito. (Giuseppina Da Ros, 2004)

En su fase inicial, las cooperativas de ahorro y crédito fueron integradas esencialmente por sectores sociales de escasos recursos económicos como obreros y pequeños artesanos.

> Con el auge de los años sesenta y el enfoque de "soporte al desarrollo rural" que le dio la Alianza para el Progreso, las cooperativas de ahorro y crédito que surgieron en esa década empezaron a ser integradas por campesinos y, por ende, ubicadas en áreas rurales. De ahí que, en 1964, el 37.4% de las cooperativas abiertas (legalizadas y en proceso de formación), registradas en la respectiva Federación (FECOAC), estaban clasificadas como rurales. Sin embargo, las cooperativas rurales representaban tan sólo un quinto del total de capital social y depósitos, por lo que su relevancia económica al interior del movimiento era escasa. (Giuseppina Da Ros, 2004)

En las siguientes décadas, sin embargo de los intentos del gobierno y de instituciones internacionales, el cooperativismo de ahorro y crédito adquiere una orientación exclusivamente urbana, enfocada a sectores sociales pertenecientes a la clase media y media-alta.

Aunque, los datos estadísticos son insuficientes, se puede observar que el sector medio urbano ha venido paulatinamente adquiriendo nuevo y mayor espacio en el transcurso de esos años, sobre todo a partir del período de bonanza creado por el auge petrolero en 1972.

Entre los factores que pueden haber impulsado el movimiento cooperativo de ahorro y crédito hacia una orientación predominantemente urbana, cabe señalar los siguientes:

- El modelo cooperativo adoptado por el movimiento de ahorro y crédito ecuatoriano que retomando las conductas y procedimientos de las CreditUnions norteamericanas, fomentó el sentido individualista y competitivo de dichas organizaciones y las condujo a actuar como bancos comerciales.
- Las crecientes oportunidades de inversión en áreas urbanas.
- Las características de los potenciales socios urbanos respecto a los rurales, en cuanto a nivel de ingreso, propensión al ahorro, monto de préstamos demandados, utilización del crédito, etc.

El sistema Cooperativo de Ahorro y Crédito ha demostrado una evolución continua y sostenida, a través de las organizaciones: a nivel mundial, la Organización Mundial de Cooperativas de Ahorro y Crédito (WOCCU, por sus siglas en inglés), a nivel Latinoamericano, la Confederación Latinoamericana de Cooperativas de Ahorro y Crédito (COLAC) y a nivel nacional la Federación Nacional de Cooperativas de Ahorro y Crédito (FECOAC).

2.1.2.3 Las Cooperativas de Ahorro y Crédito en lo Económico y Financiero

Frente a la inestabilidad y crisis del sistema bancario nacional donde el cliente ha demostrado su desconfianza, en especial en los bancos, ha sido

necesario encontrar alternativas que permitan fomentar el ahorro y brindar créditos.

Dicha alternativa es el sector de la economía solidaria, específicamente el sistema cooperativo de Ahorro y Crédito, el mismo que promueve los principios de solidaridad, ayuda mutua, autogestión y control democrático.

Las cooperativas de ahorro y crédito se constituyen en un sistema paralelo al bancario, enfocado en brindar apoyo a artesanos, pequeños productores agrícolas, comerciantes minoristas, obreros de toda clase, cuyas condiciones económicas les impiden ser sujetos de crédito en las entidades bancarias.

La importancia del sistema cooperativo se debe en gran medida a tres aspectos fundamentales como son:

- Es la fuente de crédito más importante para las microempresas
- Tiene una gran perspectiva de crecimiento hacia los sectores donde normalmente el resto de entidades financieras no llegan por la localización geográfica y los costos operativos.
- Llegan a sectores de bajos recursos en contraste con otros sectores del sistema financiero.

Las cooperativas tienen como objetivo fundamental de su actividad, el desarrollo del hombre, para cumplir con su misión requieren modernizarse y ser manejadas con conocimientos técnicos, para brindar los servicios de una manera eficiente, efectiva y económica.

Las cooperativas se caracterizan por la democratización de capitales, de ahorros y de crédito, por lo tanto no existe vinculación ni concentración de

recursos en pocas manos, que es una práctica común en las entidades bancarias.

La quiebra de varios bancos ha dado lugar al fortalecimiento del sistema cooperativo de ahorro y crédito, por cuanto se ha demostrado confianza por la solvencia de las mismas.

2.2 Desarrollo del Marco Legal y Regulatorio de las Instituciones Financieras

Durante la década de los noventa, la regulación bancaria y la consideración de que las tasas de interés eran inflexibles a disminuir debido a la falta de competencia en el sistema financiero, dio como resultado la consecuente apertura indiscriminada de bancos y financieras sin tomar en cuenta el tamaño del mercado y los costos operativos que esto genera, lo que resultó en un incremento de las tasas de interés debido a que tanto los bancos como las otras entidades financieras trataron de captar depósitos mediante la oferta de tasas de interés pasivas más altas. En enero de 1999, con la puesta en marcha del impuesto sobre la circulación de capitales que sustituyó al impuesto a la renta, disminuyó la intermediación financiera y los bancos experimentaron serios problemas de liquidez, debiendo el Estado asumir al 72% del sistema financiero a un costo aproximado de más de 4.000 millones de dólares, (Naranjo: 2004).

La iliquidez de los bancos se vio agravada porque la racionalidad económica de los ecuatorianos se manifestó en la conversión a dólares de sus ingresos provocando la dolarización informal y por la desconfianza para

realizar depósitos en esas instituciones. Como alternativa, la población consideró que las Cooperativas de Ahorro y Crédito eran el espacio seguro para entregar sus recursos económicos, y para éstas, ocurrió un efecto de crecimiento a través de la captación de dinero. (Gutiérrez Nut, 2009)

Lo expuesto derivó en un crecimiento porcentual de depósitos en las cooperativas de ahorro, por lo que la oferta de crédito también fue mayor.

Estos acontecimientos y la implementación del proceso de dolarización formal en el país, han exigido cambios en el Sistema Financiero Nacional, como respuesta para asegurar la sostenibilidad de las organizaciones financieras, evitando sus quiebras, y para garantizar que los ciudadanos no pierdan sus ahorros. En 1985, la Junta Monetaria mediante Resolución Nº JM-266-85, determina que deben formar parte del Sistema Financiero Nacional las cooperativas de ahorro y crédito consideradas como abiertas, ya partir de aquí se inicia el fortalecimiento del control de las instituciones que hacen intermediación financiera por parte de la Superintendencia de Bancos y Seguros. Para ejercer la supervisión del sistema bancario, la Superintendencia de Bancos del Ecuador recuerda que el costo de una eficiente supervisión bancaria es realmente alto, mientras que el costo de una supervisión pobre ha probado ser mayor, de tal manera que orientada por esta filosofía, cumple con los acuerdos de organismos internacionales como el Comité de Basilea, el Banco de Pagos Internacionales, el Fondo Monetario Internacional y el Banco Mundial, expresados en los “Principios de Basilea” con el fin de fortalecer la estabilidad financiera mundial y que son los siguientes:

- Principio 1. Precondiciones para una supervisión bancaria efectiva

- Principios 2 al 5: Otorgamiento de licencias y estructura
- Principios 6 al 15: Normativa y requerimientos prudenciales
- Principios 16 al 20: Métodos para la supervisión bancaria en la marcha
- Principio 21: Requerimientos de información
- Principio 22: Poderes formales de los supervisores, y
- Principios 23 al 25: Banca Fronteriza.

Guiados por los Principios Básicos para una Supervisión Bancaria Efectiva del Comité de Basilea, en la Cumbre del G-7 en Lyon, año 1996, examinaron las formas para fortalecer la estabilidad financiera en todo el mundo, fundamentadas en los principios básicos y en un compendio de recomendaciones, guías y estándares, las cuales fueron presentadas para aprobación de los Ministros de Finanzas del G-7 y del G-10 en preparación para la cumbre de Denver en junio de 1997, con la participación de representantes del Comité de Basilea, de Chile, China República Checa, Hong Kong, México, Rusia, Tailandia, Argentina, Brasil, Corea, Hungría, India, Indonesia, Malasia, Polonia y Singapur. Las guías para efectuar este trabajo deben ser cumplidas por las autoridades supervisoras y otras públicas en todos los países a nivel internacional, y están encaminadas a promover estabilidad macroeconómica y financiera global.

Para el cumplimiento de este acuerdo, los países se comprometen a realizar cambios sustantivos en el esquema legal y en los poderes de los supervisores en vista de que algunos no tienen autoridad para instrumentar los Principios, y de que el sistema bancario ejerce un rol central de sistema de

pagos y de movilización de y distribución de ahorros, por tanto deben promover un sistema competitivo y eficiente que responda a las necesidades del público de servicios financieros de buena calidad a costos razonables.

En la aplicación de los Principios, se menciona la presentación de garantías, la calificación de nuevas instituciones que justificarán tener accionistas apropiados, suficiente fortaleza financiera, estructura legal compatible con su estructura operacional y un cuerpo gerencial con suficiente experiencia e integridad para operar el banco de manera sana y prudente, la demostración de transparencia, el principio de los “cuatro ojos” que consiste en segregación de funciones, revisiones cruzadas, control dual de los activos, dobles firmas, etc., el análisis de riesgos por el incumplimiento de una contraparte con el contrato estipulado, por la concentración de créditos en pocas personas, o por el riesgo país, de mercado, de tasas de interés, de liquidez, operacional o legal. En referencia al otorgamiento de préstamos recomienda establecer un sistema de información gerencial que provea datos que alerten la existencia de créditos problema para lo cual deberían diseñar políticas de concesión de préstamos y de mantenimiento de la calidad de las garantías, la limitación de préstamos relacionados y definición de políticas estrictas de “conocimiento del cliente” a fin de evitar la asociación o relación con traficantes de drogas u otros elementos que puedan causar daño a la institución .

Además recomienda hacer una eficiente administración de la liquidez mediante el análisis de los requerimientos netos de fondeo y elaboración de planes de contingencia.

Las Cooperativas de Ahorro y Crédito realizan operaciones de intermediación financiera que permiten captar los recursos del ahorro y direccionarlos hacia créditos de consumo, vivienda, comercial y microcrédito que generen riqueza para el país. Por lo expuesto, las COACs se han convertido en un sector importante de la economía solidaria así como del sector financiero pues en varios frentes compiten con las instituciones bancarias.

2.3 Marco Regulatorio del Sector Cooperativista de Ahorro y Crédito

El 30 de septiembre de 1937 se expide la primera Ley de Cooperativas y un año más tarde, el 9 de febrero de 1938, el Reglamento General respectivo

En 1963 se emite la Ley General de Cooperativas que se reforma en 1966 y en el mismo año se emite el respectivo Reglamento.

El artículo 7 de esta Ley determina que exclusivamente el Ministerio de Bienestar Social tiene competencia para estudiar y aprobar los estatutos de todas las cooperativas que se organizan en el país, así como para concederles personería jurídica y registrarlas, aunque la Junta Monetaria en 1985, mediante resolución JM-266-85, reconoce a las “cooperativas abiertas” como aquellas cuyos estatutos indican que los socios tienen vínculos comunes con ciertos gremios, actividad económica y organización y además son entes de intermediación financiera, por tanto deben ser controladas por la Superintendencia de Bancos y Seguros. Para darle soporte jurídico a esta resolución de la Junta Monetaria, en 1992, la Dirección General de Cooperativas emite la Resolución No. DGC – 92-098 para disponer que las

COAC abiertas al público cuyos activos sean iguales o superiores a 20.000 salarios mínimos vitales, deben ser controladas por la Superintendencia de Bancos.

En 1994 es emitida la Ley General de Instituciones del Sistema Financiero. Aquí se ratifica la inclusión de las COAC abiertas al público en el Sistema Financiero Nacional.

En 1998 mediante Decreto Ejecutivo No. 1227 se emite el Reglamento de Constitución, Organización, Funcionamiento y Liquidación de las COAC abiertas.

Luego de la crisis bancaria que soportaba el país y la adopción del sistema de dolarización, en el año 2001 mediante Decreto Ejecutivo No. 2132, se deroga el Reglamento de 1998 y se establece el procedimiento para la incorporación de las COAC bajo la supervisión de la Superintendencia de Bancos y Seguros a aquellas que registran un capital social superior a US$ 200.000,00 y se fija el coeficiente de capital (relación entre el patrimonio técnico y la suma ponderada de riesgo de los activos contingentes)en 12% (para los bancos es el 9%).

En julio de 2005 mediante Decreto Ejecutivo No. 354, se deroga el Decreto Ejecutivo No. 2132 y las reformas emitidas en Decreto Ejecutivo No. 3050 del año 2002 y se establece el Reglamento que rige la constitución, organización, funcionamiento y liquidación de las cooperativas de ahorro y crédito que realizan intermediación financiera con el público, así como las cooperativas de segundo piso, sujetas al control de la Superintendencia de Bancos y Seguros, “con el fin de ejercer un efectivo control de este numeroso

conjunto de instituciones, que generalmente carecen de una adecuada gestión y dotar a este sector de un instrumento jurídico adecuado que propicie su fortalecimiento y garantice la protección de los intereses del público, mecanismo por el cual irán incorporándose gradualmente al control de aquellas instituciones que reúnan los requisitos reglamentarios y cumplan con las normas expedidas por la Junta Bancaria"[4]

Como resultado de todos estos cambios y modificaciones legales, la gestión del control de las cooperativas de ahorro y crédito en el Ecuador se cumple desde dos instancias: la Dirección Nacional de Cooperativas, entidad adscrita al Ministerio de Inclusión Económica y Social, que califica la legalidad de la conformación de las cooperativas y controla a aquellas cuyos activos son inferiores a un millón de dólares y depósitos del público menores a doscientos mil dólares norteamericanos y la Superintendencia de Bancos y Seguros, que controla a aquellas que superaron estos valores, las cuales deben ser administradas con características similares al de las entidades bancarias.

2.3.1 La Ley de Economía Popular y Solidaria

El Art. 311 de la Constitución de la República del Ecuador aprobada en el año 2008, menciona textualmente: "El sector financiero popular y solidario se compondrá de cooperativas de ahorro y crédito, entidades asociativas o solidarias, cajas y bancos comunales, cajas de ahorro. Las iniciativas de servicios del sector financiero popular y solidario, y de las micro, pequeñas y medianas unidades productivas, recibirán un tratamiento diferenciado y

[4] Boletín de Cooperativas de Ahorro y Crédito & Microfinanzas, Superintendencia de Bancos y Seguros, septiembre 2005

preferencial del Estado, en la medida en que impulsen el desarrollo de la economía popular y solidaria”

Lo expuesto modifica radicalmente el escenario de supervisión y control de las Cooperativas de Ahorro y Crédito, pues se las ubica como parte del sector financiero popular y solidario, enfocadas a brindar servicios en favor del crecimiento de las entidades y personas involucradas en la economía popular y solidaria

El 10 de mayo de 2011 se publica en el Registro Oficial la Ley de Orgánica de Economía Popular y Solidaria y el Sector Financiero Popular y Solidario, dicha ley establece los lineamientos normativos para el funcionamiento y regulación de varios actores de la economía popular y solidaria entre los que se incluye, a las Cooperativas de manera general, las cuales son clasificadas en base a su actividad en los siguientes tipos:

Cooperativas de producción.- Son aquellas en las que sus socios se dedican personalmente a actividades productivas lícitas, en una sociedad de propiedad colectiva y manejada en común, tales como: agropecuarias, huertos familiares, pesqueras, artesanales, industriales, textiles.

Cooperativas de consumo.- Son aquellas que tienen por objeto abastecer a sus socios de cualquier clase de bienes de libre comercialización; tales como: de consumo de artículos de primera necesidad, de abastecimiento de semillas, abonos y herramientas, de venta de materiales y productos de artesanía.

Cooperativas de vivienda.- tienen por objeto la adquisición de bienes inmuebles para la construcción o remodelación de viviendas u oficinas o la ejecución de obras de urbanización y más actividades vinculadas con éstas en beneficio de sus socios.

Cooperativas de ahorro y crédito.- Son organizaciones formadas por personas naturales o jurídicas que se unen voluntariamente con el objeto de realizar actividades de intermediación financiera y de responsabilidad social con sus socios y, previa autorización de la Superintendencia, con clientes o terceros con sujeción a las regulaciones y a los principios reconocidos en la presente ley.

Cooperativas de servicios.- Son las que se organizan con el fin de satisfacer diversas necesidades comunes de los socios o de la colectividad, los mismos que podrán tener la calidad de trabajadores, tales como: trabajo asociado, transporte, vendedores autónomos, educación y salud.

Dentro de este contexto es importante señalar que la nueva regulación determina un esquema normativo y de control para todas las cooperativas de ahorro y crédito. Por tanto, en el futuro cercano la nueva Superintendencia de Economía Popular y Solidaria será la encargada de la supervisión de todas las cooperativas de ahorro y crédito que prestan servicios en el Ecuador, esto incluye aquellas que hoy se encuentran bajo la supervisión de la Dirección Nacional de Cooperativas y la Superintendencia de Bancos y Seguros.

Dado que la aplicación de la Ley Orgánica de Economía Popular y Solidaria y el Sector Financiero Popular y Solidario se encuentra aún en

proceso, el país todavía no cuenta con el esquema normativo (resoluciones emitidas por la Junta de Regulación del Sector Financiero Popular y Solidario) así como los mecanismos operativos, tecnológicos y humanos que permitan garantizar su cumplimiento por parte de las entidades del sector cooperativista de ahorro y crédito.

Por tal motivo y hasta que las nuevas instituciones creadas por la Ley Orgánica de Economía Popular y Solidaria y el Sector Financiero Popular se encuentren totalmente operativas se continúa con el esquema de control que se ha venido aplicando por parte de la Superintendencia de Bancos y Seguros, así como por la Dirección Nacional de Cooperativas las cuales se encuentran en funciones prorrogadas. A dicha conclusión llegamos luego de revisar la mencionada ley que en su disposición transitoria duodécima menciona: "Hasta que las instituciones públicas que se crean en la presente Ley, se encuentren operativas, continuarán interviniendo las actuales instituciones, en funciones prorrogadas al amparo de las normas legales por las que fueron creadas. Para el caso de las cooperativas bajo control de la Superintendencia de Bancos y Seguros, en la transición el marco de la regulación será el existente a la fecha de vigencia de la presente Ley."

2.3.2 Cooperativas Reguladas por la Superintendencia de Bancos y Seguros

La Superintendencia de Bancos, persona jurídica de derecho público, es un organismo técnico y autónomo, dirigido y representado por el Superintendente de Bancos. Tiene a su cargo la vigilancia y el control de las instituciones del sistema financiero público y privado, así como de las

compañías de seguros y reaseguros y todas aquellas que se encuentran determinadas en la Constitución y en la Ley.[5]

Al 31 de julio del 2012, existen en el país 39 cooperativas controladas por las Superintendencia de Bancos y Seguros las cuales se presentan en la tabla No.1.1

[5] Presidencia de la República del Ecuador, Reglamento a la Ley General de Instituciones del Sistema Financiero - Decreto Ejecutivo No. 1852. RO/ 475 - 4 de julio de 1994

No.	Nombre Institución	Activos	Resultados
1	JUVENTUD ECUATORIANA PROGRESISTA	USD 486.867	USD 2.262
2	JARDIN AZUAYO	USD 276.008	USD 3.183
3	29 DE OCTUBRE	USD 243.720	USD 2.187
4	COOPROGRESO	USD 216.366	USD 1.498
5	MEGO	USD 179.204	USD 1.134
6	OSCUS	USD 168.573	USD 1.523
7	RIOBAMBA	USD 163.829	USD 1.378
8	SAN FRANCISCO	USD 149.422	USD 1.896
9	MUSHUC RUNA	USD 123.762	USD 1.782
10	CACPECO	USD 119.425	USD 2.038
11	ANDALUCIA	USD 105.416	USD 1.015
12	EL SAGRARIO	USD 95.200	USD 1.228
13	15 DE ABRIL	USD 92.164	USD 316
14	ALIANZA DEL VALLE	USD 89.222	USD 1.583
15	ATUNTAQUI	USD 87.419	USD 862
16	23 DE JULIO	USD 85.189	USD 1.312
17	CODESARROLLO	USD 79.151	USD 339
18	CAMARA DE COMERCIO DE AMBATO	USD 78.940	USD 1.124
19	SANTA ROSA	USD 71.409	USD 237
20	PABLO MUÑOZ VEGA	USD 65.559	USD 965
21	CACPE BIBLIAN	USD 65.231	USD 728
22	TULCAN	USD 62.934	USD 1.346
23	SAN JOSE	USD 57.068	USD 374
24	CACPE PASTAZA	USD 53.565	USD 607
25	CONSTRUCCION COMERCIO Y PRODUCCION LTDA.*	USD 47.324	USD 271
26	CACPE LOJA	USD 37.989	USD 211
27	CHONE LTDA	USD 31.724	USD 335
28	COMERCIO	USD 31.186	USD 352
29	PADRE JULIAN LORENTE	USD 29.493	USD 144
30	11 DE JUNIO	USD 24.776	USD 89
31	GUARANDA	USD 22.016	USD 127
32	SAN FRANCISCO DE ASIS	USD 20.225	USD 306
33	COTOCOLLAO	USD 18.501	USD 240
34	SAN PEDRO DE TABOADA	USD 15.088	USD (132)
35	CALCETA	USD 11.250	USD 264
36	LA DOLOROSA	USD 10.659	USD 100
37	COOPAD	USD 9.352	USD (131)
38	9 DE OCTUBRE	USD 8.215	USD 31
39	SANTA ANA	USD 7.264	USD 40

Tabla 1.1 Cooperativas de Ahorro y Crédito Supervisadas por la SBS

Las mencionadas instituciones mantienen a nivel nacional alrededor de 400 puntos de atención al cliente, entre los que se encuentran: más de 270 agencias; 39 sucursales y 18 cajeros automáticos, entre otros. Más del 50% de estos puntos se encuentran repartidos en cuatro provincias, Pichincha, Azuay, Loja y Tungurahua[6].

2.3.3 Tamaño de las Cooperativas Controladas por la SBS

La Superintendencia de Bancos y Seguros del Ecuador, tomando como referente la participación de los activos con respecto al total del sistema, de acuerdo a la metodología de percentiles, clasifica a las instituciones en cuatro grupos: entidades grandes (las que superan el 6% de los activos del sistema financiero), medianas (entre 3 y 5,99%), pequeñas (entre 1 y 2,99%) y muy pequeñas (menor a 0.99%). La tabla 1.2 muestra las cooperativas de ahorro y crédito ubicadas en su respectivo grupo de acuerdo a su tamaño:

[6]Superintendencia de Bancos y Seguros, Dirección Nacional de Estudios e Información - Comportamiento del Sistema de Cooperativas de Ahorro y Crédito, marzo del 2012

GRANDES	MEDIANAS	PEQUEÑAS	MUY PEQUEÑAS
JUVENTUD ECUATORIANA PROGRESISTA	COOPROGRESO	15 DE ABRIL	COMERCIO
JARDIN AZUAYO	MEGO	EL SAGRARIO	CHONE LTDA
29 DE OCTUBRE	RIOBAMBA	23 DE JULIO	SAN FRANCISCO DE ASIS
	OSCUS	CODESARROLLO	GUARANDA
	SAN FRANCISCO	ATUNTAQUI	11 DE JUNIO
	CACPECO	ALIANZA DEL VALLE	COTOCOLLAO
	ANDALUCIA	CAMARA DE COMERCIO DE AMBATO	LA DOLOROSA
	MUSHUC RUNA	SANTA ROSA	COOPAD
		PABLO MUÑOZ VEGA	CALCETA
		CONSTRUCCION COMERCIO Y PRODUCCION LTDA.	9 DE OCTUBRE
		TULCAN	SANTA ANA
		CACPE BIBLIAN	SAN PEDRO DE TABOADA
		SAN JOSE	
		CACPE PASTAZA	
		PADRE JULIAN LORENTE	
		CACPE LOJA	
TOTAL: 3	TOTAL: 8	TOTAL: 16	TOTAL: 12

Tabla 1.2 Tamaño de las COACs Supervisadas por la SBS

Las instituciones financieras anteriormente mencionadas se encuentran obligadas a cumplir con la normativa emitida por la Junta Bancaria y la SBS misma que se detalla en la Codificación de Resoluciones del Sistema Financiero. Como ya se mencionó anteriormente la SBS es la encargada de supervisar el cumplimiento de la normativa legal por parte de las instituciones financieras bajo su control, esto incluye las cooperativas de ahorro y crédito. Cabe señalar que todas estas acciones buscan precautelar los intereses de socios y clientes de las mencionadas entidades.

2.4 El Control en las Cooperativas de Ahorro y Crédito Supervisadas por la SBS

En el estudio que nos ocupa, haremos referencia al contenido de la Codificación de Resoluciones de la Junta Bancaria y la SBS, pues es la normativa que establece los controles para el funcionamiento de las instituciones financieras en nuestro país, siendo su cumplimiento de carácter obligatorio.

La Codificación de Resoluciones de la SBS y Junta Bancaria, es un documento dinámico que se compone de tres libros que corresponden a:

- Libro I: Sistema Financiero
- Libro II: Sistema Seguros Privados
- Libro III: Sistema Seguridad Social

Es el primer libro que contiene la normativa aplicable para el sector financiero y por lo tanto nos centraremos en él. Dicho libro se compone de 26 títulos que son los temas globales de la normativa, éstos a su vez se subdividen en capítulos, los mismos que agrupan secciones las cuales contienen a los artículos que definen de forma más detallada los requerimientos regulatorios.

En este punto es necesario dirigir el análisis hacia dos temas fundamentales para toda institución financiera (para nuestro caso las cooperativas de ahorro y crédito). Estos son el control interno y la administración de riesgos.

2.4.1 El Control Interno

En 1992, el Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO, por sus siglas en inglés) en su publicación denominada Control Interno - Marco Integrado, define al control interno de la siguiente forma: "El control interno es un proceso, efectuado por el consejo de administración, la dirección y demás personal de una entidad, diseñado para facilitar una seguridad razonable respecto de la consecución de objetivos en las siguientes categorías":

- Eficacia y eficiencia de las operaciones
- Fiabilidad de la información financiera
- Cumplimiento de leyes y normas aplicables

El control interno es muy importante para cualquier organización y más aún para una entidad financiera. Por tal motivo la Codificación de Resoluciones de la Junta Bancaria y la SBS, dedican el título XIII a este tema. Se consideran los temas más importantes para promover un esquema que permita a las instituciones financieras conseguir los objetivos planteados.

Es claro que la Codificación de Resoluciones cuenta con una gran cantidad de artículos y disposiciones para la administración de las entidades financieras, sin embargo nosotros nos concentraremos en aquellas partes que se relacionen directamente con la función a tomarse en cuenta en este proyecto: la auditoría.

Bajo este criterio y luego de haber revisado la normativa señalada, se identificó el artículo 3 de la sección I.- De la Evaluación y Recomendaciones sobre el Control Interno de la Institución del Sistema Financiero, que textualmente señala: "Los auditores internos deberán, en el curso de sus actividades anuales, cubrir una parte significativa de los negocios y actividades de la institución vigilada y al menos las siguientes:

- 3.1 Supervisar las operaciones de la institución del sistema financiero con base a un programa general de las auditorías a realizar, estructurado de acuerdo con las necesidades de la institución. La naturaleza y profundidad de la auditoría requerida dependerá del tipo y complejidad de las actividades realizadas por la institución controlada;

- 3.2 Verificar que no se den prácticas que favorezcan a los socios, directores o administradores de la entidad que pudieren constituir un menoscabo para el interés de los depositantes;
- 3.3 Promover la existencia de una cultura de control en toda la institución que favorezca una operación con adecuados estándares de seguridad; y,
- 3.4 Verificar que se cumplan las políticas, normas y procedimientos de la institución y se observen las leyes, normas y reglamentos vigentes, con el propósito de asegurar que no se infrinja la normatividad vigente".

Por lo detallado, se asigna al área de Auditoría Interna la responsabilidad directa de promover y apoyar el diseño, aplicación y mejora del sistema de control interno de las instituciones financieras controladas por la SBS.

2.4.2 La Administración de Riesgos

Mediante resolución No JB-2004-631 de 22 de enero del 2004, la Junta Bancaria incluyó el capítulo I.- "De la Gestión Integral y Control de Riesgos" como parte integrante del título X.- "De la Gestión y Administración de Riesgos", el mismo que trata sobre la normativa para la Administración del Riesgo de las Instituciones Financieras supervisadas por la SBS.

A continuación se detallan algunos artículos importantes para comprender el enfoque dispuesto por el ente de control y como su aplicación afecta a las Cooperativas de Ahorro y Crédito.

En la sección l "Alcance y Definiciones", artículo número 2, en sus puntos 2.1, 2.2 y 2.9la resolución proporciona las siguientes definiciones:

- **Riesgo**.- Es la posibilidad de que se produzca un hecho generador de pérdidas que afecten el valor económico de las instituciones;
- **Administración de riesgos**.- Es el proceso mediante el cual las instituciones del sistema financiero identifican, miden, controlan / mitigan y monitorean los riesgos inherentes al negocio, con el objeto de definir el perfil de riesgo, el grado de exposición que la institución está dispuesta a asumir en el desarrollo del negocio y los mecanismos de cobertura, para proteger los recursos propios y de terceros que se encuentran bajo su control y administración
- **Riesgo operativo**.- Es la posibilidad de que se produzcan pérdidas debido a eventos originados en fallas o insuficiencia de procesos, personas, sistemas internos, tecnología, y en la presencia de eventos externos imprevistos. Incluye el riesgo legal pero excluye los riesgos sistémico y de reputación.
- Agrupa una variedad de riesgos relacionados con deficiencias de control interno; sistemas, procesos y procedimientos inadecuados; errores humanos y fraudes; fallas en los sistemas informáticos; ocurrencia de eventos externos o internos adversos, es decir, aquellos que afectan la capacidad de la institución para responder por sus compromisos de manera oportuna, o comprometen sus intereses;

En la sección III "Responsabilidad de la Administración de Riesgos", en el artículo 9, asigna al directorio como responsable de la Administración de Riesgos, incluyendo en el punto 9.1 y como parte de sus responsabilidades lo siguiente: "Asegurarse que la auditoría interna verifique la existencia y cumplimiento del esquema de la administración integral de riesgos de la institución;"

Mediante resolución No JB-2005-834 de 20 de octubre del 2005, la Junta Bancaria incluye capítulo V.- "De la Gestión del Riesgo Operativo" dentro del título X.- "De la Gestión y Administración de Riesgos". Dicho capitulo menciona detalla las definiciones y requerimientos considerados para administrar el riesgo operativo en las instituciones financieras.

Se establece por ejemplo que el riesgo operativo se origina en base a cuatro factores que son:

- Procesos
- Personas
- Tecnología de Información
- Eventos Externos

Adicionalmente, se establece los controles y medidas de seguridad que permitan a la entidad financiera, el prevenir o responder ante un evento que implique una afectación significativa para la institución financiera. Las mencionadas salvaguardas se organizan en base a los cuatro factores del riesgo operativo.

El artículo 13, de la sección III.- Administración del Riesgo Operativo, señala: "El esquema de administración del riesgo operativo de las instituciones controladas debe estar sujeto a una auditoría interna efectiva e integral, por parte de personal competente, debidamente capacitado y operativamente independiente."

Es claro entonces que la normativa asigna a la auditoría interna la responsabilidad de realizar revisiones respecto al esquema de administración de riesgo operativo. Para cumplir con dicho encargo es necesario que la institución cuente con auditores capacitados y competentes en las áreas de gestión de procesos, administración de personal, tecnología de información y análisis de contingencias.

2.4.3 La Auditoría Interna

El artículo 1, de la sección I, De la Calificación, Requisitos y Registro, del Capítulo II.- Normas Para la Calificación de los Auditores Internos de las Entidades Sujetas al Control de la Superintendencia de Bancos y Seguros, del título XXI - De las Calificaciones Otorgadas por la Superintendencia de Bancos y Seguros, sección I, De la Calificación, Requisitos y Registro; señala: "Toda unidad de auditoría interna debe contar con un servicio de auditoría de sistemas de información, que colabore en el logro de sus funciones y objetivos. Este servicio debe contar con personal competente y experiencia específica en auditoría de sistemas, acorde con la complejidad y tamaño de las operaciones que realiza la institución del sistema financiero (incluido con resolución No. JB-2010-1549 de 21 de enero del 2010)"

Este artículo nos da la idea de la importancia que tiene la auditoría de sistemas para el ente regulador y las propias instituciones financieras. En este caso se exige a las instituciones financieras contar con un servicio de Auditoría de Sistemas que apoye las revisiones de Auditoría Interna.

De igual forma, dentro de las funciones del auditor interno se menciona en el numeral 9.3 lo siguiente: "Evaluar los recursos informáticos y sistemas de información de la institución del sistema financiero, con el fin de determinar si son adecuados para proporcionar a la administración y demás áreas de la institución, información oportuna y suficiente que permita tomar decisiones e identificar exposiciones de riesgo de manera oportuna y cuenten con todas las seguridades necesarias;"[7] Dichas evaluaciones deben ser realizadas por personal experimentado en el tema, por lo que necesariamente se requiere profesionales formados en Auditoría Informática, con experiencia en temas tales como riesgo tecnológico, control interno, gestión tecnológica, seguridad de información, gestión de proyectos, procesos de negocio, entre otros. Adicionalmente, el contar con un buen bagaje de conocimientos técnicos ayuda mucho.

Como conclusión final del presente capítulo, podemos señalar que las Evaluaciones de Auditoría Informática se han constituido en los últimos años en una herramienta fundamental para el trabajo de la función de Auditoría Interna

[7]Codificación de Resoluciones de la SBS, Libro I. Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero, Titulo xxi.- De las calificaciones otorgadas por la superintendencia de bancos y seguros, capítulo ii.- normas para la calificación de los auditores internos de las entidades sujetas al control de la superintendencia de bancos y seguros, sección iii.- definición de la auditoría interna, funciones del Auditor interno y plan de trabajo del auditor interno

en las entidades financieras controladas por la SBS. De igual manera, el trabajo del auditor tecnológico constituye un insumo valioso para la alta dirección con el fin de conocer de forma objetiva e independiente el estado del control interno y la administración de riesgos generados por los procesos de tecnología de la información.

Por lo expuesto, la SBS mediante la codificación de resoluciones, ha dispuesto la inclusión de la Auditoría de Sistemas dentro del esquema de evaluación y mejora del Control Interno, evaluación del riesgo operativo y validación de la información de las instituciones financieras, entre ellas las Cooperativas de Ahorro y Crédito. En este caso el alcance de la Auditoría de sistemas sobrepasa lo especificado por la normativa de riesgo operativo, extendiéndose a las áreas definidas por la Auditoría Interna tradicional.

Es claro, que para las 39 cooperativas supervisadas por la SBS, se ha creado la necesidad de contar con el aporte del trabajo de la Auditoría Informática, tanto para cumplir con los requerimientos regulatorios cuanto para mejorar sus controles y administración de riesgos; lo que deriva en una mejora del servicio para socios y clientes de dichas entidades.

La necesidad mencionada en el párrafo anterior nos lleva a comprender que se ha creado un gran compromiso para los profesionales de auditoría informática, pues de su trabajo dependerá que la Cooperativa pueda cumplir con el marco regulatorio, así también que pueda identificar y tratar oportunamente los riesgos derivados de la gestión tecnológica.

Con el fin de proveer de un paquete de herramientas que apoye a los auditores de sistemas informáticos en el cumplimiento de su misión en las

Cooperativas de Ahorro y Crédito supervisadas por la SBS, se ha desarrollado el presente manual de Auditoría de Sistemas, el mismo que se constituye en un aporte enfocado a mejorar la evaluación de la gestión tecnológica y los riesgos asociados a ésta.

CAPÍTULO 3

MARCO TEÓRICO

3.1 Introducción

Con el fin de establecer la estructura conceptual para el desarrollo de la presente investigación, detallaremos varias normas, marcos de trabajo y buenas prácticas desarrollados por organismos especializados en temas tales como: auditoría de sistemas, gestión de riesgos, gobierno de tecnología de información y control interno. La revisión y análisis de dichos documentos, se constituye en la base teórica considerada en el diseño y desarrollo de una propuesta para el proceso de auditoría informática enfocado a Cooperativas de Ahorro y Crédito.

Adicionalmente, se requiere ahondar en los conceptos y terminología clave relacionada con la función de Auditoría Informática, sus principios, objetivos, responsabilidades, entre otros. En este punto enfatizaremos en la importancia que tiene el Manual de Auditoría Informática dentro del trabajo del Auditor Tecnológico.

3.2 El Control Interno y su Evolución

En 1985, con el patrocinio conjunto de las cinco organizaciones profesionales más prestigiosas con sede en Estados Unidos: American Accounting Association (AAA), el Instituto Americano de Contadores Públicos

Certificados (AICPA), Financial Executives International (FEI), el Instituto de Auditores Internos (IIA), y la Asociación Nacional de Contadores (ahora el Instituto de Contadores Administrativos [IMA]); se crea la National Commission of Fraudulent Financial Reporting, conocida también como la Comisión Treadway. Dicha comisión nace con el fin de lograr dos objetivos principales como son:

- Identificar las causas atribuibles a la presentación de información financiera fraudulenta por parte de las empresas cotizantes en bolsa. Dada a conocer como parte del publicitado caso Watergate, mismo que derivó en la renuncia del entonces presidente de Estados Unidos, Richard Nixon.
- Emitir recomendaciones orientadas a minimizar la incidencia de dichas actuaciones en la economía estadounidense.

La comisión emitió varias recomendaciones relacionadas al sistema de control interno de las empresas. Se otorgó una gran importancia a temas como el entorno de control, los códigos de conducta, la formación y funcionamiento de un comité de auditoría y la aplicación de una auditoría interna activa y objetiva.

Adicionalmente, la comisión solicitó a las organizaciones patrocinadoras que se unieran en el desarrollo de un marco conceptual común de control interno, el mismo permitiría establecer una base de referencia con guías generales que apoyen a las empresas que cotizaban en bolsa en el mejoramiento y evaluación de sus sistemas de control interno.

3.2.1 Coso I

En septiembre de 1992, el Comité de Organizaciones Patrocinadoras de la Comisión Treadway denominado COSO[8]; emitió un informe mediante el cual proporciona las definiciones relativas al control interno. De igual manera dicho documento establece criterios que pueden ser usados para evaluar los controles internos de una organización. La traducción del Informe COSO fue elaborada por la firma Coopers & Lybrand y el Instituto de Auditores Internos, Capítulo España, y fue publicada en1997.

El informe de COSO, denominado Control Interno - Marco Integrado, define al control interno como un proceso efectuado por la junta directiva, la gerencia y otro personal de una entidad, diseñado para proporcionar seguridad razonable respecto al logro de objetivos en las tres categorías siguientes:

a. Eficacia y eficiencia de las operaciones,

b. Confiabilidad de la información financiera

c. Cumplimiento de leyes y regulaciones.

También identifica cinco componentes interrelacionados para lograr un control interno eficaz.

1. Entorno del control
2. Evaluación de riesgos
3. Actividades de control
4. Información y comunicación
5. Supervisión (Monitoreo)

[8] De la denominación en inglés: The Committee of Sponsoring Organizations of the Treadway Commission

La figura 3.1 muestra la interacción entre los componentes de control interno.

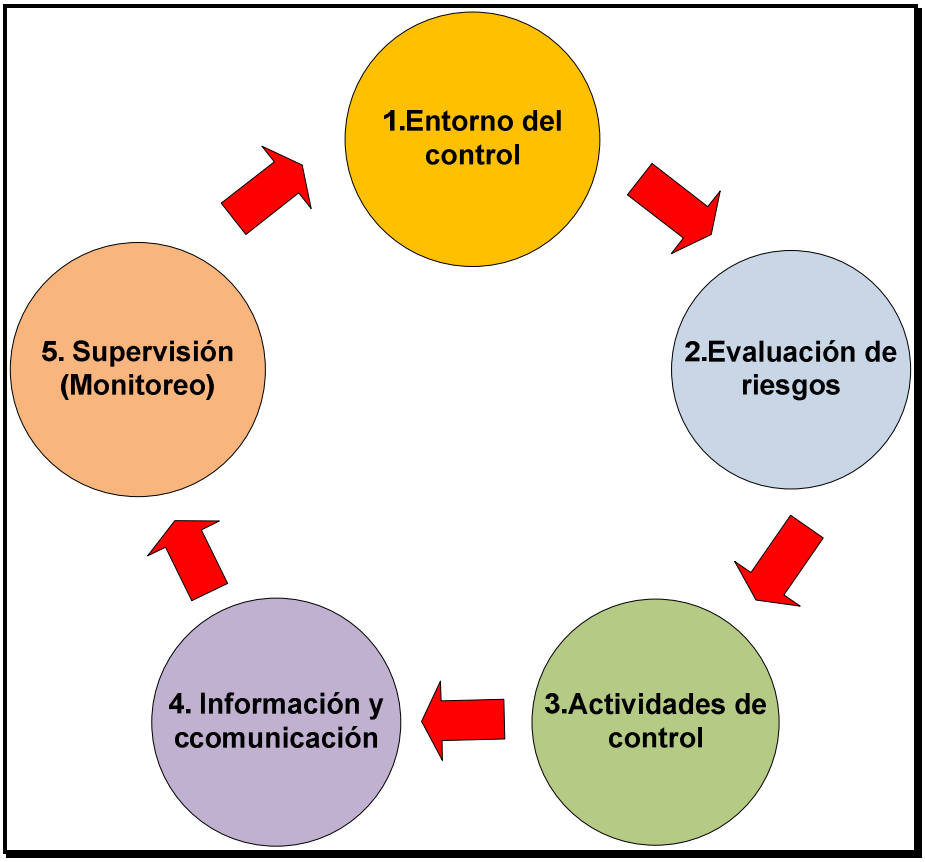

Figura 3.1 Componentes de Control Interno

3.2.2 Coso Erm

Una vez publicado, Control Interno - Marco Integrado, tuvo gran éxito convirtiéndose en un elemento de referencia fundamental para el logro de los objetivos organizacionales dentro de un marco de control interno.

En los años siguientes ha tomado un gran impulso la tendencia que define a la administración de riesgos como una pieza clave de la creación de valor para los grupos de interés de las organizaciones. Por lo mencionado, COSO desarrolló un marco de trabajo integrado a la gestión de riesgos corporativos, el mismo que busca facilitar los conceptos y principios más importantes, definiendo un lenguaje común y una orientación clara. En septiembre de 2004, COSO emite el informe denominado “Gestión de Riesgos Corporativos-Marco Integrado” conocido también como COSO - ERM, el mismo fue traducido al idioma español por la firma Pricewaterhouse Coopers y la Federación Latinoamericana de Auditores Internos (FLAI), siendo publicada dicha versión en diciembre del 2005.

La gestión de riesgos corporativos es un proceso efectuado por el consejo de administración de una entidad, su dirección y restante personal, aplicado en la definición de la estrategia y en toda la entidad y diseñado para identificar eventos potenciales que puedan afectar a la organización y gestionar sus riesgos dentro del riesgo aceptado, proporcionando una seguridad razonable sobre el logro de objetivos[9], en las siguientes categorías:

a. Estratégico (esta categoría no estaba incluida en COSO I).
b. Eficiencia y efectividad de las Operaciones
c. Confiabilidad de la Información.
d. Cumplimiento.

[9]COSO-ERM - Gestión de Riesgos Corporativos-Marco Integrado (2004)

3.2.2.1 Componentes de Coso ERM

Al igual que Coso I, Coso ERM también cuenta con sus componentes, los cuales en este caso son ocho:

1. **Ambiente interno**: La dirección fija una filosofía respecto al riesgo y determina el riesgo aceptado. El ambiente interno establece la base de cómo el personal de la empresa debe percibir y afrontar el control y el riesgo. El núcleo de cualquier negocio está constituido por sus personas – con sus atributos individuales, incluyendo integridad, valores éticos y competencia- y el entorno en el que actúan.

2. **Establecimiento de objetivos**: Los objetivos deben existir antes de que la dirección pueda identificar los eventos potenciales que afectan a su consecución. La gestión de riesgos corporativos asegura que la dirección ha establecido un proceso para fijar objetivos y que los objetivos seleccionados apoyan la misión de la entidad y se alinean con ella, además de ser consistentes con el riesgo aceptado.

3. **Identificación de eventos**: Deben identificarse los eventos potenciales que pueden tener un impacto en la entidad. Esto implica la identificación de posibles acontecimientos internos o externos que afectan a la consecución de objetivos, diferenciándolos según su procedencia, e incluye la distinción entre los que representan riesgos u oportunidades o ambas circunstancias a la vez. Las oportunidades se reenvían hacia la estrategia de la dirección o a los procesos para fijar objetivos.

4. **Evaluación de riesgos**: Los riesgos identificados se analizan para formar una base que determine cómo deben gestionarse y se asocian a los objetivos a los que pueden afectar, evaluándose desde la doble perspectiva de riesgo inherente y residual y considerando tanto su probabilidad como su impacto.

5. **Respuesta a los riesgos**: El personal identifica y evalúa las posibles respuestas a los riesgos: evitar, aceptar, reducir o compartir. La dirección selecciona un conjunto de acciones para poner en línea los riesgos con sus tolerancias respectivas y el riesgo aceptado por la entidad.

6. **Actividades de control**: Las políticas y procedimientos se establecen y ejecutan para asegurar que se llevan a cabo eficazmente las respuestas a los riesgos seleccionadas por la dirección.

7. **Información y comunicación**: La información relevante se identifica, capta y comunica de un modo y en un plazo que permita a las personas desarrollar sus responsabilidades. Hace falta información a todos los niveles de una entidad para identificar, evaluar y responder a los riesgos. También puede darse una comunicación eficaz en sentido amplio, cuando fluye en todas direcciones dentro de la entidad. El personal debe recibir comunicaciones claras sobre su papel y responsabilidades.

8. **Supervisión**: Toda la gestión de riesgos corporativos se supervisa, realizando en ella las modificaciones que sean necesarias. De este modo, se puede reaccionar dinámicamente y cambiar si varían

las circunstancias. Esta supervisión se lleva a cabo a través de actividades permanentes de la dirección, evaluaciones independientes de la gestión de riesgos corporativos o una combinación de ambas actuaciones.

Como podernos observar, la gestión de riesgos se constituye en un proceso estrechamente relacionado con el control interno de una organización. Es claro que el establecimiento de un sistema de gestión de riesgos efectivo permitirá desarrollar y mejorar los controles de la empresa, procurando la consecución de sus objetivos.

Basándonos en lo señalado por el componente número 8 denominado Supervisión, observamos que se considera necesario realizar evaluaciones independientes (es decir auditorías) al sistema de gestión de riesgos, esto con el fin de tratar las posibles desviaciones generadas por los constantes cambios tanto internos como externos a la organización. He aquí la importancia para las organizaciones de toda índole, en el caso que nos compete las Cooperativas de Ahorro y Crédito; el contar con herramientas que les permitan a sus áreas de Auditoría Interna realizar las evaluaciones citadas anteriormente.

3.2.3 Cobit4.1

En el año de 1998 el IT Governance Institute fue establecido con el fin de evolucionar el pensamiento y los estándares internacionales correspondientes al direccionamiento y control de la tecnología de información

en las organizaciones. Este organismo señala que un efectivo gobierno de TI[10] ayuda a la empresa a asegurar que se consiguen los siguientes objetivos específicos:

- Garantizar que TI soporta las metas de negocio
- Optimizar la inversión del negocio en TI
- Administrar de forma adecuada los riesgos y oportunidades relacionadas con TI

Dentro de este esquema el ITGI desarrolló una publicación titulada Objetivos de Control para la Información y la Tecnología Relacionada (COBIT 4.1), la cual se constituye en un recurso educacional enfocado hacia directores ejecutivos de información, directores generales y profesionales de administración y control de TI.

La misión de Cobit se orienta a investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento[11].

Bajo el concepto de que el Gobierno de TI es responsabilidad de los ejecutivos, del consejo de directores y consta de liderazgo, estructuras y procesos organizacionales enfocados a garantizar que TI sostiene y entiende las estrategias y objetivos organizacionales; podemos identificar un enfoque

[10]Tecnología de Información
[11]Cobit 4.1

similar al propuesto por COSO I y COSO ERM. Adicionalmente, COBIT 4.1 va más allá, pues integra e institucionaliza las mejores prácticas para asegurar que TI soporta los objetivos del negocio.

Por lo mencionado, Cobit 4.1 se constituye en un marco referencial para control de TI, mismo que es soportado principalmente por seis estándares mundiales relacionados con TI, entre los cuales se encuentran: COSO I, COSO ERM, además de ITIL[12], ISO/IEC 27000, CMM[13] y CMMI[14], PMBOK[15] y El estándar de buenas prácticas para la seguridad de la información propuesto por el ISF[16].

3.2.3.1 Estructura de Cobit 4.1

Cobit 4.1 se caracteriza por brindar buenas prácticas mediante un marco de trabajo estructurado por dominios y procesos, complementario a esto presenta las actividades en una estructura lógica y manejable. Es necesario señalar que las mejores prácticas consignadas por Cobit 4.1 constituyen el consenso de los expertos y se hallan orientadas más fuertemente al control y menos a la ejecución. Este marco de trabajo se constituye en una referencia para comparar la situación de una organización cuando se percibe que su administración de TI tiene dificultades.

[12] ITIL: Biblioteca de Infraestructura de TI
[13] CMM: Modelo de madurez de la capacidad
[14] CMMI: Integración del modelo de madurez de la capacidad
[15] Guía para el Cuerpo de Conocimiento de Gestión de Proyectos
[16] Foro de Seguridad de Información

Es importante para la empresa que sus requerimientos de negocio sean soportados adecuadamente por la función de TI, para lograr dicho propósito Cobit 4.1 propone una serie de prácticas que satisfacen esta necesidad de la siguiente manera:

a. Estableciendo un vínculo con los requerimientos del negocio

b. Organizando las actividades de TI en un modelo de procesos generalmente aceptado

c. Identificando los principales recursos de TI a ser utilizados

d. Definiendo los objetivos de control gerenciales a ser considerados (evaluados)

Uno de los temas fundamentales observados por Cobit es la orientación hacia el negocio, como podemos ver en la figura 3.2, para proporcionar la información requerida por la empresa para cumplir sus objetivos, es necesario que la organización invierta, controle y administre los recursos de TI mediante un esquema estructurado de procesos.

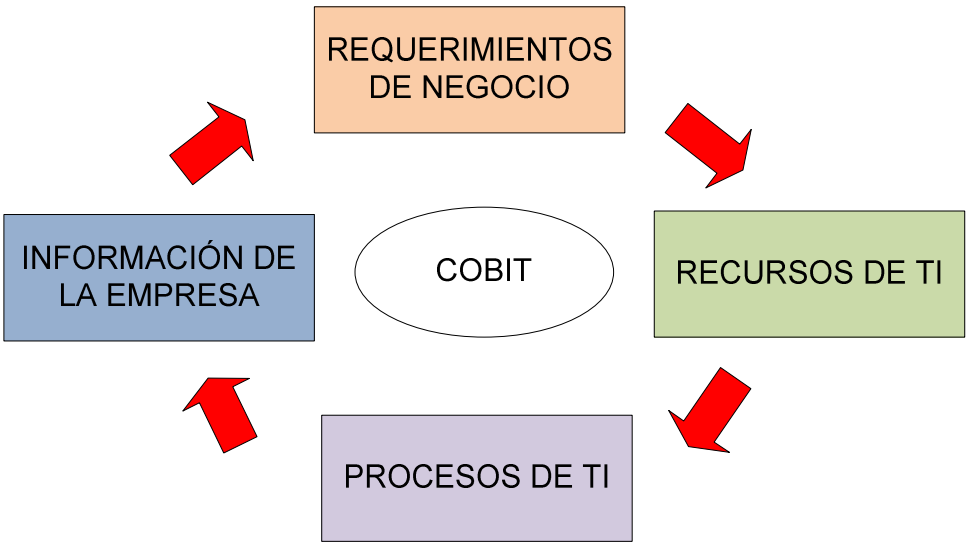

Figura 3.2 Principio básico de Cobit (Cobit 4.1, 2007)

Cobit está conformado por 34 procesos los cuales se organizan en cuatro dominios que se detallan a continuación:

a. Planear y Organizar (PO): Proporciona dirección para la entrega de soluciones (AI) y la entrega de servicio (DS)

b. Adquirir y Evaluar (AI): Proporciona las soluciones y las pasa para convertirlas en servicios.

c. Entregar y Dar Soporte (DS): Recibe las soluciones y las hace utilizables por los usuarios finales.

d. Monitorear y Evaluar (ME): Monitorear todos los procesos para asegurar que se sigue la dirección provista.

En la figura3.3 se aprecia la interrelación entre los cuatro dominios de Cobit.

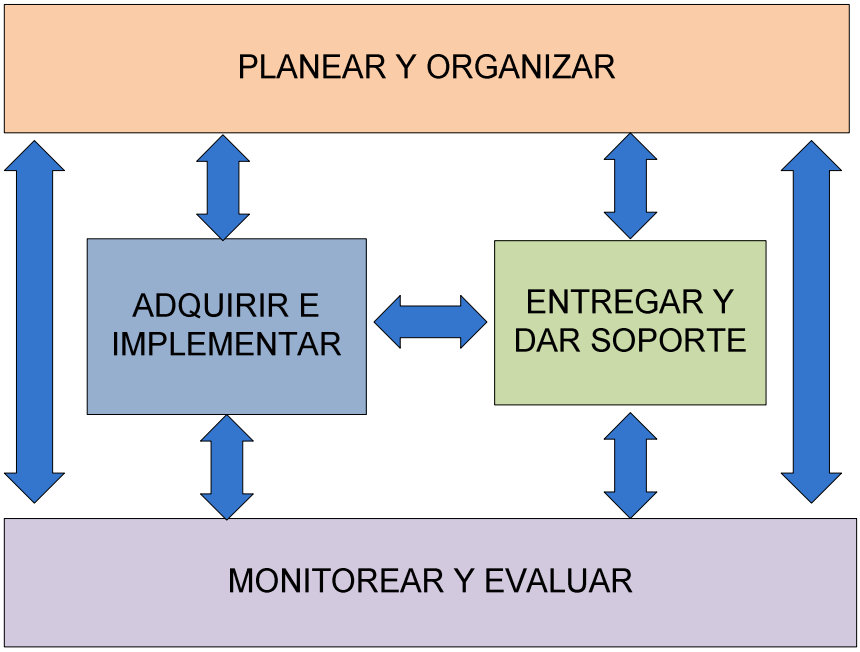

Figura 3.3 Dominios Interrelacionados de Cobit (Cobit 4.1, 2007)

Adicionalmente en la tabla 3.1 podemos observar la lista de procesos del modelo Cobít 4.1 organizados en los cuatro dominios descritos.

DOMINIO	PROCESO
PLANEAR Y ORGANIZAR	PO1 Definir un Plan Estratégico de TI
	PO2 Definir la Arquitectura de la Información
	PO3 Determinar la Dirección Tecnológica
	PO4 Definir los Procesos, Organización y Relaciones de TI
	PO5 Administrar la Inversión en TI
	PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia
	PO7 Administrar Recursos Humanos de TI
	PO8 Administrar la Calidad
	PO9 Evaluar y Administrar los Riesgos de TI
	PO10 Administrar Proyectos
ADQUIRIR E IMPLEMENTAR	AI1 Identificar soluciones automatizadas
	AI2 Adquirir y mantener software aplicativo
	AI3 Adquirir y mantener infraestructura tecnológica
	AI4 Facilitar la operación y el uso
	AI5 Adquirir recursos de TI
	AI6 Administrar cambios
	AI7 Instalar y acreditar soluciones y cambios
ENTREGAR Y DAR SOPORTE	DS1 Definir y administrar los niveles de servicio
	DS2 Administrar los servicios de terceros
	DS3 Administrar el desempeño y la capacidad
	DS4 Garantizar la continuidad del servicio
	DS5 Garantizar la seguridad de los sistemas
	DS6 Identificar y asignar costos
	DS7 Educar y entrenar a los usuarios
	DS8 Administrar la mesa de servicio y los incidentes
	DS9 Administrar la configuración
	DS10 Administrar los problemas
	DS11 Administrar los datos
	DS12 Administrar el ambiente físico
	DS13 Administrar las operaciones
MONITOREAR Y EVALUAR	ME1 Monitorear y Evaluar el Desempeño de TI
	ME2 Monitorear y Evaluar el Control Interno
	ME3 Garantizar el Cumplimiento Regulatorio
	ME4 Proporcionar Gobierno de TI

Tabla 3.1 Lista de Procesos Cobit 4.1 (Cobit 4.1, 2007)

3.2.3.1.1 ¿Qué es un proceso?

Un proceso es un conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados[17]. En la figura 3.4 se muestra la estructura conceptual de un proceso, se muestra las entradas que sirven de insumo, el proceso representado por las actividades que toman las entradas y con ayuda de los recursos (financieros, tecnológicos, humanos, entre otros) las transforman en un resultado o producto. Cabe indicar que para obtener un producto deseado las actividades deberán cumplir con varios requerimientos los cuales son representados por los controles.

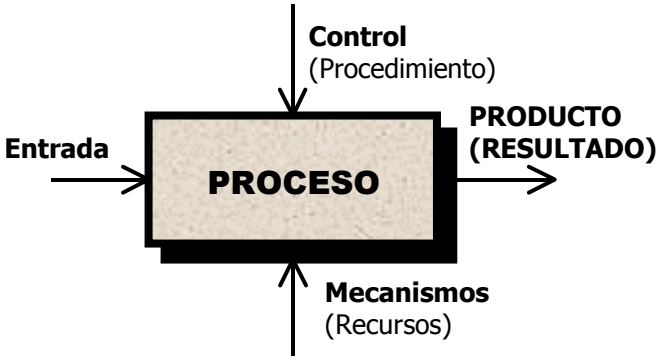

Figura 3.4 Estructura conceptual del proceso

Cabe señalar que el esquema de procesos COBIT brinda un modelo de procesos genéricos que representa todos los procesos que normalmente se encuentran en las funciones de TI, brindando un modelo de referencia común comprensible para los gerentes operativos de TI y del negocio.

[17] Norma ISO 9000:2005

3.2.3.1.2 Los Recursos de TI

Como ya mencionamos anteriormente, los procesos requieren de recursos de diversos tipos para lograr ejecutarse y brindar los resultados esperados.

En caso de Cobit requerimos de una gama de recursos de TI, cuya administración adecuada permitirá adicionalmente a una operación efectiva de los procesos empresariales una efectiva administración de las inversiones en tecnología.

Los recursos de TI, identificados por Cobit se han agrupado en cuatro categorías que se describen a continuación:

1. **Aplicaciones:** incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.
2. **Información:** son los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información, en cualquier forma en que sean utilizados por el negocio.
3. **Infraestructura:** es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.
4. **Personas:** son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar

los sistemas y los servicios de información. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran.

3.2.3.1.3 Los Controles[18]

El control es definido como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos.

Cobit plantea una colección de objetivos de control de TI que agrupan un conjunto completo de requerimientos de alto nivel a tomar en cuenta por parte de la gerencia para conseguir un control efectivo de cada proceso de TI. Estos controles presentan las siguientes características:

- Son recomendaciones de acciones de gerencia para aumentar el valor y/o reducir el riesgo
- Consisten en políticas, procedimientos, prácticas y estructuras organizacionales.
- Son diseñadas con el fin de proporcionar un aseguramiento razonable de que los objetivos empresariales se conseguirán y que los eventos no deseables serán prevenidos, detectados y corregidos.

La gerencia de la organización requiere adoptar decisiones relativas a estos objetivos de control, para lo cual deberá cumplir con los siguientes pasos:

[18]Cobit 4.1

- Seleccionar aquellos aplicables.
- Decidir aquellos que deben implementarse.
- Elegir la forma de implementarlos (frecuencia, extensión, automatización, etc.)
- Aceptar el riesgo de no implementar aquellos que podrían aplicar.

Para conseguir un gobierno efectivo, la gerencia deben implementar los controles necesarios considerando un marco de control definido para todos los procesos TI. Puesto que los objetivos de control de TI de COBIT se encuentran organizados por procesos, el marco de trabajo especifica los vínculos entre los requerimientos de gobierno de TI, los procesos de TI y los controles de TI.

3.2.3.1.4 Aceptabilidad General de COBIT

COBIT se fundamenta en el análisis e integración de varios estándares y mejores prácticas de TI, adaptándose a principios de gobierno corporativo generalmente aceptados. Se encuentra posicionado a alto nivel en la estructura administrativa de la organización, impulsado por los requerimientos del negocio, cubre completamente las actividades de TI, y se enfoca en lo que se debe lograr en lugar de como lograrlo, para conseguir un gobierno, administración y control efectivos.

Es importante señalar que por su condición de integrador de prácticas de gobierno de TI, Cobit se traduce en un marco de interés para varios actores de la gestión tecnológica tale como: la dirección ejecutiva; la gerencia del

negocio, la gerencia y gobierno de TI; los profesionales de aseguramiento y seguridad; así como para los profesionales de auditoría y control de TI.

La implantación de las mejores prácticas debe ser consistente con el gobierno y el marco de control de la empresa, debe ser adaptada para cada organización, y debe integrarse con otros métodos y prácticas que se utilicen. Los estándares y las mejores prácticas por sí mismas no nos aseguran el éxito sino, pues su efectividad depende de cómo hayan sido implementados en la realidad y de los esfuerzos que ser realicen para mantener los actualizados.

La utilidad de Cobit aumenta cuando es aplicado como un conjunto de principios que sirvan como un punto de partida para luego adaptar los procedimientos específicos. Tanto la administración como el equipo de TI deben comprender qué hacer, cómo hacerlo y su importancia para garantizar que se cumplen las prácticas del marco de trabajo.

Es recomendable que Cobit sea utilizado al más alto nivel, otorgando así un marco de control general basado en el modelo de procesos de TI (descrito anteriormente) que debe ser aplicable a toda empresa. Las prácticas y los estándares específicos que cubren áreas discretas, se pueden equiparar con el marco de trabajo de Cobit, brindando así una jerarquía de materiales guía.

A continuación describiremos los distintos usuarios, para los cuales Cobit resulta de gran importancia e interés:

- **Dirección ejecutiva**: Para obtener valor de las inversiones y para balancear las inversiones en riesgo y control en un ambiente de TI.

- **Gerencia del negocio:** Para obtener certidumbre sobre la administración y control de los servicios de TI, proporcionados internamente o por terceros
- **Gerencia de TI:** Para proporcionar los servicios de TI que el negocio requiere para dar soporte a la estrategia del negocio de una forma controlada y administrada
- **Auditores:** Para respaldar sus opiniones y/o para proporcionar asesoría a la gerencia sobre controles internos

Cobit ha sido desarrollado y es mantenido por un instituto de investigación sin ánimo de lucro, tomando la experiencia de los miembros de sus asociaciones afiliadas, de los expertos de la industria, y de los profesionales de control y seguridad. Su contenido se basa en una investigación continua sobre las mejores prácticas de TI y se le da un mantenimiento continuo, proporcionando así un recurso objetivo y práctico para todo tipo de usuario[19].

Es justo hacer énfasis en la importancia que tiene Cobit como una fuente de referencia fundamental para el trabajo de auditoría que será planteado más adelante en el presente proyecto. Obtendremos de Cobit los objetivos de control que serán probados con el fin de formar la opinión del auditor de sistemas de información sobre la entidad y/o proceso objeto de revisión.

[19] Cobit 4.1

3.2.3.2 Cobit Quickstart

Durante los años siguientes a la publicación de COBIT. el núcleo de su contenido ha mantenido una evolución permanente. Como resultado, se han desarrollado varios documentos derivados de COBIT, los cuales se han enfocado principalmente en la implementación de dicho marco de buenas prácticas, tocando temas tales como: importancia, responsabilidades, asesoría, diagnóstico y relación con otras normativas de seguridad, gestión de proyectos y gestión de servicios de TI.

Dentro de este grupo de trabajos derivados se encuentra Cobit Quickstart, el cual proporciona una línea base de control para las organizaciones más pequeñas y un posible primer paso para las grandes empresas.

COBIT Quickstart es la herramienta desarrollada con el fin de administrar y controlar la tecnología de información en las PYMES[20], COBIT Quickstart provee al igual que COBIT 4 dominios, pero a diferencia de éste que tiene 34 procesos y 210 objetivos de control, COBIT Quickstart posee solo 32 Procesos y 59 objetivos de control.(Ver tabla 3.2)

[20] PYME: La pequeña y mediana empresa

	COBIT	QUICKSTART
DOMINIOS	4	4
PROCESOS	34	32
OBJETIVOS DE CONTROL	210	59

Tabla 3.2 Comparación de Cobit Quickstart con Cobit 4.1

La idea de Cobit Quickstart es que sea utilizado por las PYMES como una herramienta para la implementación del Gobierno de TI de forma rápida y práctica, puesto que, como ya observamos anteriormente, cuenta con un conjunto menor de prácticas gerenciales y procesos, el mismo que ha sido ubicado en un formulario que sirve como punto de partida o para la implementación de gobierno de TI en la organización de estudio.

Cobit Quickstart fue desarrollado con un enfoque para empresas pequeñas y medianas con una estructura pequeña de TI, sin embargo, una organización grande puede utilizar Cobit Quickstart como un punto de partida para iniciar la implementación de Gobierno de TI.

3.2.3.2.1 Cobit Quickstart y las Pymes

Según habíamos visto anteriormente, Cobit se constituye en un conjunto completo de recursos que provee la información que las organizaciones necesitan para implementar y mantener su gobierno de TI. Sin embargo, la amplitud y profundidad de la orientación proporcionada por todos los recursos de Cobit puede ser demasiado detallada y abrumadora para las organizaciones más pequeñas. O incluso, para algunas organizaciones más grandes, Cobit

puede requerir bastante tiempo y recursos para analizar a la hora de tomar los primeros pasos hacia el gobierno de TI.

El impulso principal detrás de Cobit Quickstart es la necesidad de los administradores de TI de las organizaciones más pequeñas de lograr un modo sencillo de utilizar la herramienta, esto con el fin de agilizar la aplicación de los principales objetivos de control. De igual forma, los administradores de TI de grandes organizaciones pueden aprovechar la herramienta para "inicio rápido" de las fases iniciales de una aplicación más amplia del gobierno de TI.

En estas circunstancias, los usuarios de Cobit pueden utilizar Quickstart como una herramienta simplificada y adaptada de Cobit, así como los materiales compatibles que se proveen, los cuales son inmediatamente utilizables.

Es importante señalar que las organizaciones pueden utilizar la línea de base como está, sin modificaciones, o utilizarlo como punto de partida para construir prácticas más detalladas de gestión.

La selección del material de Cobit fue realizado observando la misma filosofía que la presentada en la Guía de implementación el Gobierno de TI, es decir tomando como partida los objetivos de negocio y el análisis de riesgo respectivo para luego pasar a apoyar las metas de TI identificando los procesos que se deben mejorar, y finalmente llegando a los objetivos de control que deben ser aplicados o mejorados.

El uso de Cobit Quickstart depende de que la organización en la cual se planea implementarlo, cuente con un grupo de condiciones (supuestos) que se detallan a continuación:

- La infraestructura de TI no sea compleja.
- Las tareas más complejas de TI sean tercerizadas.
- La meta sea menos desarrollo, más compra.
- Existan habilidades limitadas de TI internamente (poco conocimiento técnico).
- La tolerancia al riesgo sea relativamente alta.
- La empresa sea muy dada a controlar los costos.
- Exista una estructura organizacional de TI muy simple.
- Exista un alcance corto del control. (no hay suficientes procesos levantados)

Estos supuestos son representativos de la cultura de control y entorno de TI de la mayoría de las PYME y posiblemente también de algunas filiales o entidades autónomas de las organizaciones más grandes. Esto implica que el conjunto resultante de los procesos y objetivos de control es probable que sea adecuado para un entorno PYME. Adicionalmente, implica que puede ser un punto de partida para organizaciones grandes que requieran realizar un inicio rápido en la implementación de un programa de gobierno de TI. Estas organizaciones deberían ampliar su marco de gobierno en función de su actividad específica y los requisitos de gobierno determinados.

Adicionalmente, Cobit Quickstart proporciona una referencia para fines de auditoría y aseguramiento, esto nos permite considerarlo como un insumo para el proceso de auditoría de nuestro manual de auditoría para COACs; pues por su enfoque hacia PYMES se ajusta a la realidad tecnológica y organizacional de las COACs que como vimos en el capítulo 1, han sido catalogadas en su mayoría (92%) como organizaciones medianas, pequeñas y muy pequeñas.

3.2.3.2.2 Estructura de Cobit Quickstart

Quickstart se basa en una selección de los procesos y objetivos de control de Cobit 4,1. El resultado es una versión simplificada incluyendo un conjunto limitado de procesos y prácticas de gestión.

Quickstart también proporciona una hoja de ruta para planificar su implementación. Dicha hoja también puede ser utilizada como guía para aplicar todo el marco Cobit completo.

Retomando los supuestos para la aplicación de Cobit Quickstart, podemos señalar que los mismos deben ser considerados por cualquier organización que utilice Quickstart en su gobierno de TI y para el marco de control. Esto debido a que el desarrollo de control asociado con estas hipótesis implica que determinados controles, formalmente definidos en Cobit, se ejercen de manera informal pero efectiva. Por ejemplo, el control y la dirección que generalmente vienen dados por una fuerte supervisión, típica de este tipo de organizaciones, no se observan en Cobit Quickstart.

De acuerdo con la publicación completa Cobit 4.1, los controles generales y controles de proceso de aplicaciones no se abordan en el contenido detallado de Cobit Quickstart. Sin embargo, es fundamental considerar dichos controles al implementar Quickstart, pues los mismos son requeridos por la administración para tener una visión completa de todos los requisitos de control de la empresa.

Cobit Quickstart consta de 32 páginas de métricas, directrices gerenciales y matrices RACI que permiten a las PYMEs iniciar una autoevaluación de los controles implementados, si existen, y ayuda a enfocar el uso de los escasos recursos en las actividades críticas del negocio. Adicionalmente, Quickstart se presenta de una forma fácil de leer, de forma tabular y en un lenguaje no técnico, para fomentar la rápida adopción y la reducción de debates y discusiones.

Desde la perspectiva de la alta dirección, Cobit Quickstart ayuda a las organizaciones a concentrar los escasos recursos en lo básico, proporcionando así una herramienta eficiente para iniciar la gestión de gobierno de TI, sin realizar grandes cantidades de inversiones de recursos.

La primera reflexión al considerar Quickstart es decidir si es adecuado para una organización específica. Quickstart ayuda a la empresa a tomar esta decisión mediante la inclusión de herramientas que permiten a la organización llevar a cabo una auto-evaluación de los factores que definen la gestión y complejidad de TI. Para las grandes organizaciones, hay que reconocer que Quickstart sólo puede ser un punto de partida para avanzar hacia un marco más amplio de gobierno de TI.

3.2.3.2.3 Usuarios de Cobit Quickstart

Quickstart es útil para todo tipo de usuarios en sus tipos específicos de organizaciones: auditores, gerentes de TI y los implementadores de gobierno de TI para quienes es probable que lo estén realizando por primera vez y que deseen un método sencillo para empezar.

En el caso que nos compete es importante señalar que Cobit Quickstart provee una guía para el trabajo del auditor de TI, pues se trata de una herramienta que define los objetivos de control a probar así como un mecanismo para seleccionar dichos controles.

3.2.3.2.4 ¿Cómo saber si Quickstart es adecuado para mi organización?

Cobit Quickstart ofrece dos pruebas para evaluar la capacidad de una empresa para implementar el control de TI.

Prueba 1- Manteniéndose en la zona azul

La primera prueba (estancia en la zona azul), como se muestra en la figura 5, ayuda a la organización determinar si Cobit Quickstart es apropiado para gestionar sus riesgos de TI o se debería considerar el uso de la guía Cobit completa.

Si los resultados de la evaluación figuran principalmente en la zona azul, es más probable que la organización deba decidirse por el uso de Cobit Quickstart. Si los resultados no están en la zona azul, no deja de ser la decisión de la administración para utilizar el enfoque de Quickstart de todos modos. Sin embargo, la administración debe seguir siendo consciente de los supuestos de

control descritas anteriormente, ya que algunos controles no son observados por Cobit Quickstart.

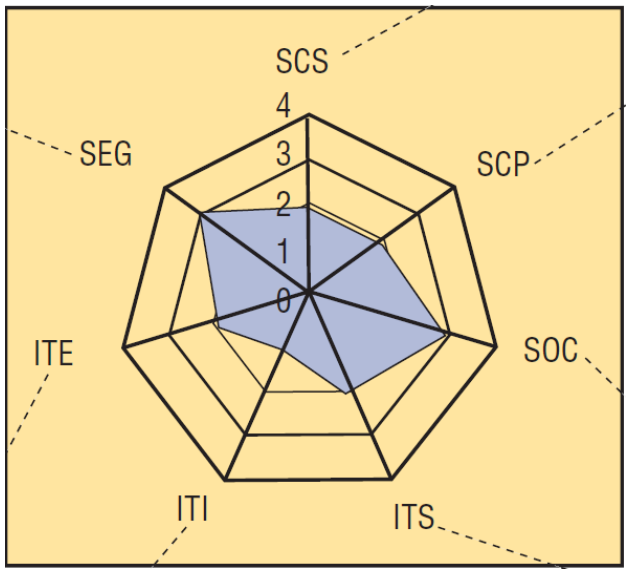

Figura 3.5 Manteniéndose en la zona azul (Cobit Quickstart, 2007)

Las diferentes dimensiones de este ensayo de aptitud son las siguientes:

1. Estructura de Mando Simple (SCS): Mide el grado en que la autoridad, las reglas y de control son institucionalizadas en la organización. Esta estructura de comando varía de muy informal y verbal estrictamente formal y documentado.

2. Sistema Corto de Comunicaciones (SCP): La trayectoria de comunicación corta indica cuántas capas se sitúan entre el jefe de la organización y el personal de TI. Esto ilustra que tan directa, rápida y eficientemente la Gerencia puede comunicarse con el personal de TI y monitorear el cumplimiento de las responsabilidades relacionadas

3. Alcance del control (SOC): Mide la influencia que tiene la Gerencia en las responsabilidades de TI. El hecho de que la Gerencia no conozca las responsabilidades de TI, al menos del personal clave es un indicador de que se requiere un marco de control más amplio.

4. Sofisticación de TI (ITS): Se refiere al comportamiento de la organización frente a la adopción de nuevas tecnologías y la complejidad del entorno de TI. Este perfil va desde ser pionero hasta ser un rezagado en la adopción de nuevas tecnologías. Un complejo entorno de TI evoca la posibilidad de mayores riesgos y requisitos de control.

5. Importancia estratégica de TI (ITI): Evalúa el grado de dependencia de la organización con respecto a TI para cumplir sus objetivos y lograr una ventaja competitiva. Si resulta que TI es fundamental para apoyar las operaciones actuales seguramente se requieren mayores controles para dicho ambiente.

6. Gastos de TI (ITE): este componente se encuentra estrechamente ligado a la sofisticación de TI y la importancia estratégica. Se evalúa y compara la inversión en TI con respecto a los beneficios recibidos y en comparación con las inversiones de otras áreas. Si el gasto de TI aumenta cada año, supera los beneficios o difiere significativamente de otras empresas del sector es prudente considerar controles más estrictos.

7. Segregación (SEG): Evalúa si las responsabilidades de operar, influir y supervisar las soluciones de TI se encuentran demasiado

concentradas en una sola persona o si por el contrario se distribuyen apropiadamente entre más personas. De darse el primer caso se produce un nivel mayor de riesgos que requiere un nivel de control mayor.

Si los resultados de la evaluación se encuentran principalmente en la zona azul, es más probable el uso de Cobit Quickstart para la organización, sin embargo, todavía puede haber circunstancias específicas que crean la necesidad de ir más allá de Quickstart (es decir, utilizar Cobit u obtener material adicional específico).

Prueba 2- Ver el Calor

La segunda prueba de la herramienta de idoneidad (Vea el calor), tal como se muestra en la figura 6 y también se suministra como parte de Cobit Quickstart, la misma que puede ayudar a evaluar las situaciones de excepción que puedan presentarse. Cuanto más la empresa esté en la zona roja, más necesita considerar que va más allá de Cobit Quickstart.

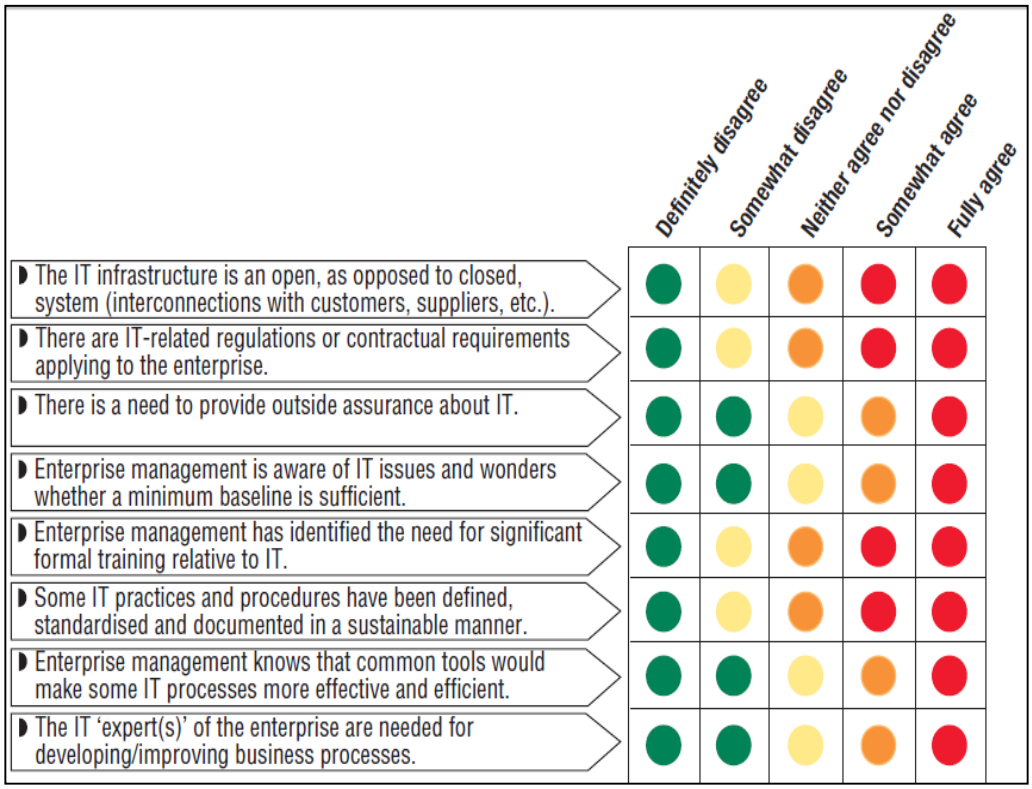

Figura 3.6 Herramienta de Calor (Cobit Quickstart, 2007)

3.2.4 Los Controles

Los controles incluyen políticas, procedimientos y prácticas (tareas y actividades) que son establecidas por la gerencia para proveer una certeza razonable de que se alcanzarán objetivos específicos[21].

3.2.4.1 Controles Generales

Los controles generales son aplicables a todas las áreas de la organización, incluyendo infraestructura y servicios de soporte de TI. Los controles generales incluyen controles internos que están principalmente dirigidos a las operaciones de contabilidad. Se refieren a la protección de

[21] Manual de Preparación al Examen CISA 2009

activos y a la confiabilidad de la información financiera de la empresa. A continuación se señalan varios tipos de controles generales:

- Controles internos de contabilidad: dirigidos principalmente hacia las operaciones contables, se relacionan con la salvaguarda de activos y la confiabilidad de los registros financieros.
- Controles operativos: se encargan de las operaciones, funciones y actividades cotidianas y aseguran que la operación esté cumpliendo los objetivos del negocio.
- Controles administrativos: se ocupan de la eficiencia operativa de un área funcional y la adherencia a las políticas de la gerencia.
- Políticas y procedimientos organizacionales de seguridad para asegurar el uso apropiado de activos de información y tecnología.
- Políticas generales para el diseño y uso de documentos y registros (manuales y automáticos) para asegurar el registro apropiado de las transacciones (pista de auditoría)
- Procedimientos y prácticas para asegurar la protección en el acceso y uso de recursos e instalaciones.
- Políticas de seguridad física y lógica para todos los centros de datos y recursos de TI.

3.2.4.2 Controles de Sistemas de Información

Los procedimientos de control general pueden ser traducidos en procedimientos de control específico para sistemas de información. Partimos de la premisa de que un sistema de información correctamente diseñado debería contar con controles integrados en el mismo sistema para todas las funciones sensibles o críticas.

Para ejemplificar lo descrito podemos citar el caso de un procedimiento general para asegurar la adecuada custodia del accesos a los activos e instalaciones, el mismo que puede traducirse en un conjunto de procedimientos de control a sistemas de información, que tome en cuenta controles de acceso a los programas de computación, datos y equipos de cómputo.

Los procedimientos de control de sistemas de información incluyen los siguientes:

- Estrategia y dirección
- Organización general y gestión
- Acceso a los recursos de TI, incluyendo datos y programas
- Metodologías de desarrollo de sistemas y control de cambios
- Procedimientos de operación
- Programación de sistemas y funciones de soporte técnico
- Procedimientos de aseguramiento de calidad
- Controles de acceso físico

- Planeación de continuidad del negocio/recuperación ante desastres
- Redes y comunicaciones
- Administración de bases de datos
- Protección y mecanismos de detección contra ataques internos y externos

Como hemos visto los controles tienen una función fundamental en la gestión del sistema de control interno, se subdividen en dos tipos y los cuales a su vez agrupan una variedad muy amplia de subtipos. Como veremos más adelante, el conocimiento de los controles es fundamental para el trabajo del auditor, pues la opinión que se haga del proceso o sistema evaluado dependerá de los resultados obtenidos de las pruebas a los controles asociados.

3.3 La Gestión de Riesgo de TI

Existen muchas definiciones de riesgo, lo cual significa que el riesgo quiere decir cosas diferentes para distintas personas. Sin embargo, a continuación citaremos las definiciones que de forma más sencilla explican lo que representa el riesgo para un ambiente empresarial y/o tecnológico.

a. Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la

organización.[22] (Definición usada en el ambiente de la seguridad de la información)

b. La posibilidad de que un evento ocurra y afecte adversamente a la consecución de objetivos.[23]

c. Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.[24]

Estas definiciones nos permiten situar al riesgo en un contexto organizacional usando los conceptos tales como pérdida, afectación, activos y objetivos empresariales, términos comprendidos fácilmente por los gerentes del negocio.

Los riesgos del negocio están relacionados directamente con la probabilidad de que las amenazas puedan explotar una vulnerabilidad, materializando el riesgo lo que produce un impacto negativo sobre un activo o grupo de activos, este hecho tiene como resultado una afectación a la empresa y la consecución de sus objetivos.

La naturaleza de las amenazas puede ser financiera, regulatoria u operacional, y puede surgir como resultado de la interacción del negocio con su ambiente, o como resultado de las estrategias, sistemas, así como tecnología, procesos, procedimientos e información usadas por el negocio.

[22] NTE INEN-ISO/IEC 27005
[23] COSO ERM
[24] MAGERIT

El trabajo del auditor de sistemas de información está a menudo relacionado con temas de alto riesgo asociados con aspectos de seguridad de información, así como con los sistemas y procesos que generan, almacenan y administran dicha información. Por tanto, es importante para los auditores de sistemas de información valorar la efectividad de los procesos utilizados para gestionar los riesgos en la organización.

El trabajo de auditoría de sistemas requiere comprender la relación existente entre riesgos y control, pues es necesario poder identificar y diferenciar los tipos de riesgo y los controles usados para mitigarlos. También es fundamental valorar el riesgo con el fin de determinar el enfoque y planear el trabajo de auditoría. Finalmente, los auditores deben entender que dentro del proceso de Auditoría también existe riesgo.

Existen varias metodologías y prácticas utilizadas para el análisis y gestión de riesgos de TI, entre las cuales tenemos:

- Risk IT (ISACA)
- ISO 27005 Gestión del riesgo en la seguridad de la información
- OCTAVE: Evaluación de amenazas y vulnerabilidades de recursos críticos operacionales (Carnegie Mellon University)
- MAGERIT: Metodología de análisis y gestión de riesgos de los sistemas de información. (Gobierno de España)

El desarrollo del presente proyecto ha tomado a Magerit como la metodología en la cual se apoyará para realizar el proceso de análisis de riesgos que formará parte del desarrollo del manual de auditoría de sistemas. Por lo expuesto, ahondaremos en la parte teórica de dicha metodología para

posteriormente utilizar esta información en la definición del proceso de auditoría de sistemas enfocado a las COACs.

3.3.1 Magerit Versión 2

MAGERIT[25] fue desarrollado por el CSAE[26] bajo la consideración de que la administración y toda la sociedad en general, dependen en gran medida de la tecnología.

La razón de ser de Magerit está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone beneficios para los ciudadanos (usuarios); pero que de igual forma da lugar a ciertos riesgos que deben ser tratados con medidas de seguridad que generen confianza en el uso de tales medios.

Magerit propone una metodología que permite a las partes afectadas por los sistemas de información, conocer el nivel de confianza que deben otorgarle a cada sistema en particular. En este punto es importante señalar que lo que se busca es conocer los riesgos de cada plataforma y/o servicio, esto con el fin de poder confiar en dichos aplicativos, así como tomar medidas para enfrentar y controlar los riesgos.

3.3.1.1 Objetivos de Magerit

Magerit busca los siguientes objetivos:

1. Directos:

[25]MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
[26]CSAE: Consejo Superior de Administración Electrónica de España

- Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de tratarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

2. Indirectos
    - Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

3.3.1.2 Análisis y Gestión de Riesgos

Magerit define estos dos conceptos complementarios y que requieren ser diferenciarlos claramente.

Como mencionamos antes, el riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema, de aquí parte el concepto del análisis de riesgos:

El análisis de riesgos: "es el proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización"

Una vez que conocemos qué podría pasar y cómo nos afecta es momento de tomar acciones sobre dicho resultado, a esto se le denomina gestionar los riesgos.

Gestión de riesgos: selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlarlos riesgos identificados.

Como parte del proceso de auditoría se empleará la parte correspondiente al análisis de riesgos, pues su resultado servirá como un insumo para enfocar y planificar las actividades de auditoría en los aspectos que representan mayor riesgo para la entidad. El ámbito de la gestión de riesgos, si bien puede ser de interés para el auditor, tiene una relación más directa con la administración de la organización que a final de cuentas es la responsable de aplicar las medidas para proteger los activos y servicios de TI.

La auditoría se sirve del análisis de riesgos (ya sea realizado por ellos mismos o por la organización) dentro de la primera fase de la revisión, esto debido a que es necesario conocer la unidad auditable a ser evaluada. Por lo tanto es muy importante para el auditor conocer los riesgos asociados con el fin de formarse una opinión sobre el nivel de control de un determinado proceso, aplicación o servicio de TI.

El análisis de riesgos es una herramienta de administración que nos ayuda a tomar decisiones, las mismas que pueden estar ligadas por ejemplo a la inversión tecnológica, despliegue de un centro de datos, implementación de medidas técnicas de seguridad, aplicación de procesos y selección y capacitación de personal, entre otros.

3.3.1.3 Proceso de Análisis de Riesgos

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo los siguientes pasos:

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación
2. Determinar a qué amenazas están expuestos aquellos activos
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo
4. estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
5. estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

En la figura 3.7 se puede observar la estructura de pasos aplicados para realizar un análisis de riesgos:

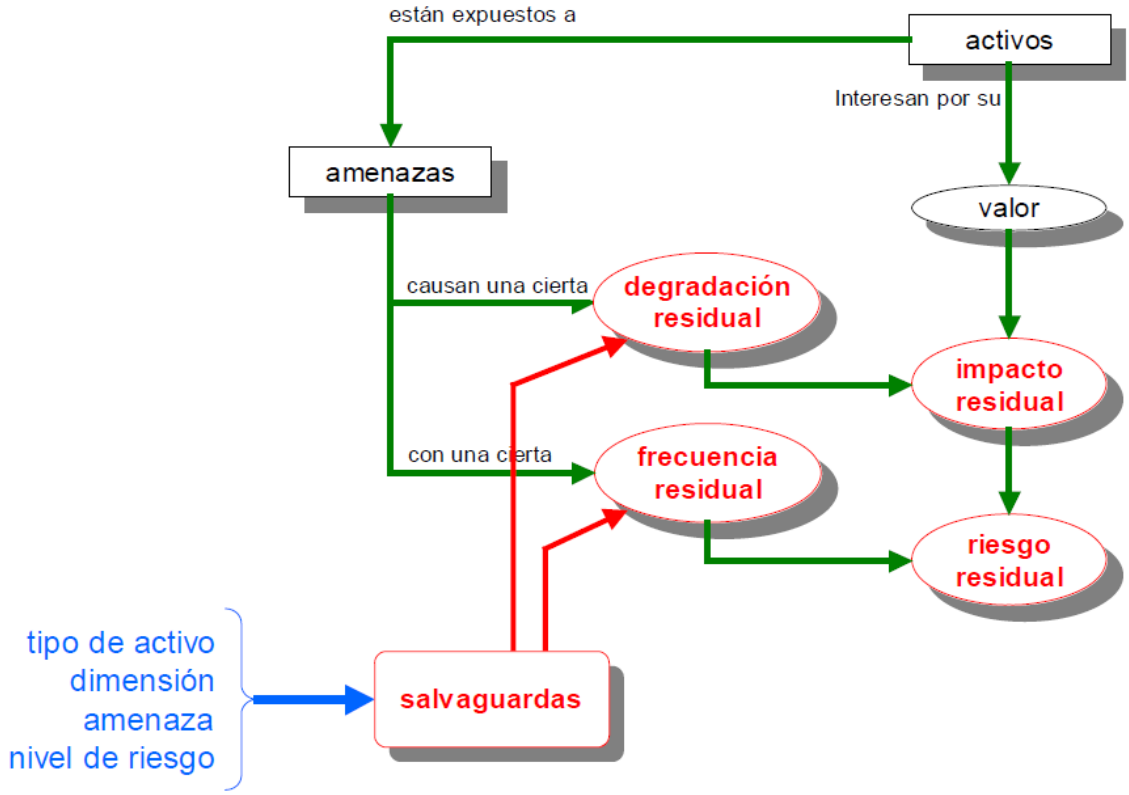

Figura 3.7 Análisis de Riesgos (Magerit, 2006)

3.4 El Proceso de Auditoría de Sistemas de Información

3.4.1 Antecedentes

Una vez que la tecnología fue direccionada hacia la sistematización de los procesos de negocio, se empezaron a desarrollar e implementar aplicaciones administrativas para contabilidad, nómina, entre otros, lo que dio como resultado que naciera la necesidad de generar un proceso de revisión del procesamiento de los aplicativos conocido como auditoría de sistemas.

Posteriormente, el uso de la tecnología cubrió las áreas del negocio en todos los niveles por medio de productos y servicios diversos; se masificó el uso de las computadoras personales, se desarrollaron las redes locales, se

produjo la interconexión empresarial por medio del avance en las telecomunicaciones, entre los principales aspectos que apuntalaron el avance tecnológico de la sociedad. Es claro que un mayor desarrollo vino acompañado de una mayor complejidad para controlar tal nivel de tecnificación, por tal motivo la auditoría informática también tuvo que evolucionar a fin de cumplir con su misión de evaluación de la gestión tecnológica.

En esta sección se aborda algunos conceptos que permiten conocer más a fondo el proceso de auditoría tecnológica y el trabajo del auditor de sistemas de información o auditor informático.

3.4.2 La Función de Auditoría Informática

3.4.2.1 Definiciones

3.4.2.1.1 Auditoría

ISACA en su Manual de Preparación al Examen CISA define a la auditoría como "un proceso sistemático por el cual un equipo o una persona calificada, competente e independiente obtiene y evalúa objetivamente la evidencia respecto a las afirmaciones acerca de un proceso con el fin de formarse una opinión sobre el particular e informar sobre el grado de cumplimiento en que se implementa dicha afirmación."

3.4.2.1.2 Clasificación de las Auditorías[27]

Dentro del ámbito de auditoría interna y externa se consideran los siguientes tipos de auditorías con sus procedimientos asociados:

[27] Manual de Preparación al Examen CISA - 2009

1. **Auditoría financiera**: Su propósito es determinar la razonabilidad de los estados financieros de una organización. A menudo este tipo de auditorías incluyen pruebas sustantivas detalladas.
2. **Auditoría operativa**: Está diseñada para evaluar la estructura del control interno en un proceso o área determinada. Las auditorías de sistemas de información sobre controles de las aplicaciones o de sistemas de seguridad lógica son ejemplos de este tipo de auditorías.
3. **Auditoría integrada**: Combina pasos de auditoría financiera y operativa. Se realiza para valorar los objetivos generales dentro de la organización, relacionados con la información financiera y la salvaguarda de activos, la eficiencia y el cumplimiento. Una auditoría integrada puede ser ejecutada por auditores externos o internos e incluye pruebas de cumplimiento a los controles internos y los pasos de auditoría sustantiva.
4. **Auditoría administrativa**: Se orientan a valorar aspectos relacionados con la eficiencia de la productividad operativa dentro de una organización.
5. **Auditoría de sistemas de información**: Es un proceso que recolecta y evalúa la evidencia para determinar si los sistemas de información y los recursos relacionados protegen adecuadamente los activos, mantienen la integridad y disponibilidad de los datos y del sistema, proveen información relevante y confiable, logran de forma efectiva las metas organizacionales, usan con eficiencia los

recursos y tienen controles internos que proveen una certeza razonable de que los objetivos de negocio, operacionales y de control serán alcanzados.

6. **Auditoría especializada**: Dentro de las auditorías de sistemas de información, existe un número de revisiones especializadas que tratan áreas reales tales como los servicios realizados por terceros. Dado que las empresas muestran una creciente dependencia de los servicios prestados por terceros, es fundamental que se evalúe los controles internos de dichos ambientes.
7. **Auditoría forense**: Se trata de una auditoría especializada en descubrir, revelar y hacer seguimiento a fraudes y crímenes. El objetivo de dicha revisión es la generación de evidencia relacionada con fraude corporativo y crimen cibernético. En los casos en que los recursos de computadora puedan haber sido mal empleados, una investigación adicional es necesaria para recopilar evidencia de posible actividad criminal que puede luego ser reportada a las autoridades competentes.

3.4.2.1.3 Auditoría Informática

La auditoría de sistemas de información se define como aquella auditoría que abarca la revisión y evaluación total o parcial de los sistemas

automatizados que procesan la información, procesos relacionados no automatizados y las interfaces entre ellos.[28]

Para realizar una auditoría, se requieren varios pasos. Entre los cuales podemos citar las siguientes:

- Planear la auditoría
- Valorar los riesgos de las áreas generales y de aplicación y servicios relacionados a auditar
- Desarrollar un programa de auditoría que comprenda objetivos y procedimientos de auditoría que satisfagan los objetivos de la auditoría
- El proceso de auditoría en el campo, el mismo que consta de actividades de recolección de evidencia y evaluación de los controles mediante la ejecución de pruebas de auditoría
- Elaboración de un reporte de auditoría que presente en forma objetiva las debilidades de control identificadas y las recomendaciones para su corrección

La gerencia de auditoría debe asegurar que exista disponibilidad de recursos de auditoría adecuados y una agenda para llevar a cabo las revisiones, en el caso de las auditorías de sistemas de información o informáticas, para cumplir con el trabajo de seguimiento de las acciones correctivas desarrolladas por la administración de la empresa.

[28] Manual de Preparación al Examen CISA 2009

3.4.2.2 Planeación de la Auditoría

La función de auditoría informática debe considerar una etapa de planificación, la cual le permita organizar los recursos de auditoría en proyectos y actividades de revisión que la lleven a cumplir con sus objetivos de ente evaluador y asesor. En el caso de las unidades de auditoría interna, es necesario cumplir con la etapa de planeación tanto de las auditorías a realizar en un periodo de tiempo (usualmente un año), así como para el desarrollo de cada auditoría individual.

3.4.2.2.1 Planeación Anual

La planeación de la auditoría está constituida tanto por la planeación a corto como a largo plazo. La planeación a corto plazo considera los aspectos relevantes de auditoría que serán cubiertos durante el año, mientras que la planeación a largo plazo toma en cuenta los riesgos originados por cambios en la dirección estratégica de la TI y que afectarán al ambiente de TI de la organización.

El análisis mencionado debe realizarse al menos una vez por año. Su utilidad va en el sentido de considerar los nuevos aspectos de control, los cambios en el ambiente de riesgo, en la tecnología, en los procesos y las técnicas mejoradas de evaluación. Los resultados de este análisis deben ser revisados por la alta dirección y aprobados por el comité de auditoría, si existiera, en el caso de las COACs, es el consejo de vigilancia quién ha venido ejerciendo dicha función.

3.4.2.2.2 Planeación de Auditorías Individuales

Adicionalmente de la planeación general anual, es necesario contar con una planeación enfocada a cada asignación individual de auditoría. Para realizar este proceso el auditor informático debe mantener un conocimiento general del ambiente a revisar, esto incluye una compresión general de las diversas prácticas del negocio y de las funciones relativas al sujeto de la auditoría, así como también los tipos de sistemas de información y la infraestructura de TI que los soporta. El auditor de TI debe conocer el marco regulatorio en el que se desarrolla el negocio.

ISACA en su Manual de Preparación al Examen CISA 2009 propone los siguientes pasos para realizar la planeación individual de auditoría:

- Entender la misión, objetivos, el propósito y los procesos del negocio, esto incluye los requisitos de información y procesamiento (disponibilidad, integridad, confidencialidad, entre otros).
- Identificar contenidos específicos tales como políticas, normas y directrices requeridas, procedimientos y estructura de la organización.
- Realizar un análisis de riesgos que ayude al diseño del plan de auditoría.
- Llevar a cabo una revisión de los controles internos relacionados con TI.
- Establecer el alcance y los objetivos de la auditoría.
- Desarrollar el enfoque o estrategia de auditoría.

- Asignar recursos humanos a la auditoría.
- Considerar la logística del trabajo de auditoría.

Cabe señalar que las leyes y regulaciones de gobierno tienen un efecto muy importante en la planeación del trabajo de auditoría interna informática. Para el caso de las COACs es indispensable tomar en cuenta lo definido por la Superintendencia de Bancos y Seguros (próximamente por la Superintendencia de Economía Popular y Solidaria), así también considerar otras leyes y normativa relacionada a temas tales como: datos electrónicos, datos personales, derechos de autor, comercio electrónico, firmas digitales, entre otros.

3.4.2.3 Marco Normativo para la Auditoría Informática (Isaca)

ISACA es una organización que agrupa a los profesionales en auditoría, control, gobierno, riesgo y seguridad de TI. Cuenta con más de 100.000 miembros y una presencia en más de 75 países a nivel mundial[29], se ha constituido como un organismo especializado en el desarrollo de estándares internacionales de auditoría y control de sistemas de información orientados a mejorar y facilitar el trabajo de los auditores de sistemas de información, profesionales de seguridad de información, riesgos y gobierno de TI.

[29] Global Network, ISACA, recuperado en noviembre 20, 2012, disponible en http://www.isaca.org/About-ISACA/History/Pages/default.aspx

ISACA ha desarrollado una estructura normativa para el desarrollo del trabajo del auditor de informático, el cumplimiento y aplicación de dichas normas es obligatorio para los miembros de esta organización profesional y más aún para aquellos profesionales que cuentan con la certificación CISA[30] (desarrollada por ISACA para aquellos profesionales que demuestran un conocimiento y aplicación más profunda de la normativa).

Adicionalmente, ISACA cuenta con material de capacitación, foros de discusión, herramientas (formales y virtuales) enfocadas en apoyar el desarrollo del trabajo de auditoría de sistemas o auditoría informática.

Toda esta estructura documental y normativa ha influenciado en gran escala el desarrollo del presente proyecto. Por tal motivo, a continuación se hace referencia a los conceptos más importantes definidos por ISACA en temas de auditoría de sistemas de información.

3.4.2.3.1 Código de Ética Profesional de Isaca

ISACA ha creado un Código de Ética Profesional con el fin de guiar la conducta profesional y personal de los miembros de su asociación y personales certificados como CISA. Este código sin embargo, debería ser aplicado por todos aquellos profesionales que desarrollan las funciones de auditoría de sistemas de información, pues dicta los requisitos de alto nivel para desarrollar la profesión. El código en mención es el siguiente:

Los miembros y los profesionales Certificados de ISACA deberán:

[30]CISA: Certified Information Systems Auditor

1. Apoyar la implementación y fomentar el cumplimiento de las normas, procedimientos y controles apropiados en los sistemas de información.
2. Ejecutar sus labores con objetividad, diligencia, y cuidado profesional, de conformidad con las normas y mejores prácticas profesionales.
3. Servir en el interés de las partes interesadas en una forma legal y honesta, y al mismo tiempo mantener altos estándares de conducta y carácter, y no involucrarse en actos que puedan desacreditar la profesión.
4. Mantener la privacidad y la confidencialidad de la información obtenida en el curso de su función a menos que la autoridad legal requiera su revelación. Dicha información no será usada para beneficio personal ni será revelada a terceros.
5. Mantener competencia en sus respectivos campos y comprometerse a emprender únicamente las actividades que se espera que puedan realizar con competencia profesional.
6. Informar a las personas adecuadas los resultados del trabajo realizado, revelando todos los hechos significativos de los que tengan conocimiento
7. Apoyar la formación profesional de las partes interesadas para mejorar su comprensión sobre seguridad y control de sistemas de información.

3.4.2.3.2 Normas de Auditoría Informática

El desarrollo de las normas para la auditoría de sistemas de información es la parte fundamental de la contribución profesional de ISACA a la comunidad de auditores. Las normas son de cumplimiento obligatorio para el desarrollo del proceso y los reportes de auditoría de sistemas de información. El profesional de auditoría de sistemas debe contemplar que pueden existir normas adicionales, o incluso requisitos legales que deben ser cumplidos por el auditor.

Las normas de auditoría informática se detallan a continuación:

- S1 Estatuto: señala que es necesario documentar en un estatuto el propósito, responsabilidad, autoridad y obligación de rendir cuentas de la función de auditoría de sistemas de información.
- S2 Independencia: requiere del auditor y la unidad de auditoría en sí, una actitud de independencia frente al área o actividad auditada, evitando las relaciones que afecten el desarrollo objetivo de la revisión.
- S3 Ética y normas profesionales: se enfoca en la necesidad de que el auditor ejerza el debido cuidado profesional, considerando las normas de auditoría aplicables.
- S4 Competencia profesional: señala que el auditor asignado a un determinado trabajo de auditoría debería contar con la preparación y conocimiento para desarrollar dicha revisión.

- S5 Planeación: define que el auditor debería planear el trabajo de auditoría en base a los objetivos de la auditoría y las leyes aplicables. Adicionalmente, debería tomar en cuenta el enfoque de auditoría basado en riesgos, así como el desarrollo y documentación del plan, el programa y los procedimientos de auditoría.
- S6 Realización de labores de auditoría: Esta norma define que el trabajo de auditoría debe contar necesariamente con una supervisión adecuada que permita asegurar los resultados. También se incluyen las consideraciones para obtención y documentación del proceso de auditoría y de la evidencia que respalde los hallazgos detectados.
- S7 Reporte: se detallan varios requerimientos para los reportes de resultados o informes de auditoría. Se requiere la inclusión de aspectos tales como: alcance, período, objetivos, tiempo y extensión del trabajo realizado, hallazgos, conclusiones y recomendaciones, así como cualquier reserva, restricción o limitación que haya afectado el alcance de la auditoría.
- S8 Actividades de seguimiento: Luego de entregar el reporte de hallazgos, el auditor debería solicitar y evaluar información que permita definir si la administración tomó acciones al respecto.
- S9 Irregularidades y acciones ilegales: Se definen varias condiciones que deben ser consideradas por el auditor referente a los actos irregulares y/o ilegales. Se requiere considerar la

posibilidad de declaraciones falsas motivadas por este tipo de actos ilegales. Es necesario obtener conocimiento de la organización, su ambiente de control interno, seleccionar y probar los controles y el riesgo de que la gerencia no los respete.

- Adicionalmente, el auditor de sistemas de información debería desarrollar las acciones que le permitan identificar aquellos casos en que el personal conoce o sospecha del cometimiento de actos ilegales. Dichos actos una vez identificados y evaluados deben ser comunicados de forma inmediata y oportuna a los niveles adecuados dentro de la organización y a los entes reguladores correspondientes.
- S10 Gobernabilidad de TI: se define los requerimientos que el auditor de sistemas debería revisar, asociados a la función de sistemas de información y su alineación a la estrategia de la organización.
- S11 Uso de la evaluación de riesgos en la planeación de auditoría: determina que el auditor de sistemas debería utilizar una técnica o enfoque apropiado para la valoración de riesgos, esto con el fin de determinar las prioridades para asignación de los recursos de auditoría.
- S12 Materialidad de la auditoría: se refiere al hecho de que tanto la revisión como el reporte de auditoría deben considerar aquellas debilidades de control que representan afectaciones significativas para la organización.

- S13 Uso del trabajo de otros expertos: existen ocasiones en las cuales se requiere usar el trabajo de otros expertos con el fin de asegurar los resultados de la auditoría. El auditor debería estar satisfecho con los procesos de calificación profesionales, competencias, experiencia, recursos e independencia de los expertos, antes del compromiso. Adicionalmente, el auditor debe valorar si el trabajo de los expertos le permite emitir una opinión sobre los objetivos de la revisión de auditoría.
- S14 Evidencia de auditoría: el auditor de sistemas de información debe considerar la obtención de la evidencia suficiente y competente que le permita establecer las conclusiones y resultados de la auditoría.
- S15 Controles de TI: bajo esta norma el auditor de sistemas debe evaluar y monitorear los controles de tecnología de información que constituyen parte del ambiente de control interno de la organización. De igual forma debe brindar asistencia a la organización en materia de diseño, implementación y monitoreo de controles de TI.
- S16 Comercio electrónico: el auditor de sistemas debe valorar los riesgos asociados a revisiones de ambientes de comercio electrónico, el enfoque está orientado básicamente a las transacciones de dicho servicio.

3.4.2.3.3 Directrices de Auditoría Informática

El objetivo de las directrices de ISACA es brindar información adicional sobre cómo cumplir con las normas para auditoría de sistemas. En este caso el auditor informático debería:

- Considerarlas para determinar cómo implementar las normas anteriormente citadas
- Usar su propio juicio profesional para la aplicación
- Poder justificar cualquier diferencia

Las directrices desarrolladas por ISACA para la auditoría de sistemas se mencionan a continuación:

- G1 Usar el trabajo de otros auditores
- G2 Requerimiento de Evidencia de Auditoría
- G3 Uso de Técnicas de Auditoría Asistidas por Computador (CAATs)
- G4 Servicio Externo de Actividades de SI para otras organizaciones
- G5 Estatuto de Auditoría
- G6 Conceptos de Materialidad para la Auditoría de SI
- G7 Debido cuidado profesional
- G8 Documentación de Auditoría
- G9 Consideraciones de Auditoría en caso de irregularidades
- G10 Muestreo de Auditoría
- G11 Efecto de los Controles Generales de SI
- G12 Relación organizacional e Independencia

- G13 Uso de la Evaluación de Riesgos en la Planeación de Auditoría
- G14 Revisión de los Sistemas de Aplicación
- G15 Planeación Revisada
- G16 Efecto de Terceros en los controles de TI
- G17 Efecto de funciones ajenas a la Auditoría sobre la independencia del Auditor
- G18 Gobierno de TI
- G19 Irregularidades y Actos Ilegales
- G20 Informes
- G21Revisión de Sistemas de Planeación de Recursos Empresariales (ERP)
- G22 Revisión Comercio Electrónico (B2C)
- G23 Ciclo de Vida del Desarrollo de Sistemas (SDLC)
- G24 Banca por Internet
- G25 Revisión Redes Privadas Virtuales
- G26 Revisión de Proyectos de Reingeniería de Procesos (BPR)
- G27 Computación Móvil
- G28 Cómputo Forense
- G29 Revisión Post-Implementación
- G30 Competencia
- G31 Privacidad
- G32 Revisión del Plan de Continuidad de Negocio (BCP)

- G33 Consideraciones Generales para el uso de Internet
- G34 Responsabilidad de Rendir Cuentas
- G35 Actividades de Seguimiento

3.4.3 Estatuto de Auditoría

El propósito, responsabilidad, autoridad y rendición de cuentas de la función de auditoría de sistemas de información o de las asignaciones de auditoría de sistemas de información deben documentarse de manera apropiada en un estatuto de auditoría o carta de compromiso.

El estatuto de auditoría o la carta de compromiso deben ser aceptados y aprobados en el nivel apropiado dentro de la organización.

Para una función de auditoría interna de sistemas de información, se debe preparar un estatuto de auditoría para las actividades permanentes. El estatuto de auditoría debe someterse a una revisión anual, o con mayor frecuencia si varían o cambian las responsabilidades.

El auditor interno de SI puede utilizar una carta de compromiso para aclarar o confirmar su participación en tareas específicas de auditoría o de no auditoría. Para el caso de una auditoría externa de SI, normalmente debe prepararse una carta de compromiso para cada tarea de auditoría o de no auditoría.

El estatuto de auditoría o la carta de compromiso deben ser lo suficientemente detallados como para comunicar el propósito, la responsabilidad y las limitaciones de la función o de la auditoría asignada.

El estatuto de auditoría o la carta de compromiso deben revisarse periódicamente para garantizar que el propósito y la responsabilidad hayan sido documentados.

Con el fin de obtener información adicional sobre la preparación de un estatuto de auditoría o una carta de compromiso, se debe consultar las Directrices de Auditoría de SI G5, Estatuto de auditoría.

3.4.4 Auditoría Basada en Riesgos

Cada día, más y más organizaciones están adoptando el método de la auditoría basada en riesgos, éste se usa para valorar los riesgos y para apoyar a la decisión del auditor de TI de realizar ya sean pruebas de cumplimiento o pruebas sustantivas. Es importante señalar que la auditoría basada en riesgos apoya eficientemente al auditor a determinar la naturaleza y la extensión de las pruebas.

Cuando se aplica una metodología de auditoría basada en riesgos, el auditor no sólo se basa en el riesgo, sino también en los controles internos y operativos, así también en su conocimiento de la empresa o del negocio. Todas estas actividades le permiten realizar selecciones prácticas de las pruebas que se van a realizar.

Los riesgos del negocio constituyen preocupaciones originadas en los probables efectos que un evento incierto podría tener en el logro de los objetivos organizacionales. El origen de estos riesgos puede ser financiero, regulatorio u operativo y puede abarcar riesgos asociados con tecnologías específicas. Por ejemplo, en el caso de una compañía de aviación que se halla sujeta a extensas y fuertes regulaciones de seguridad y a cambios económicos

que afectan en la continuidad de sus operaciones; la disponibilidad de los servicios de TI es crítica.

Una vez que el auditor de sistemas de información o tecnológico comprende la naturaleza del negocio, puede identificar y clasificar los tipos de riesgo que definirán el modelo de riesgo o la metodología para llevar a cabo la auditoría. La valoración del riesgo puede ir desde ponderar los tipos de riesgo del negocio e identificar los riesgos en una ecuación hasta desarrollar esquemas donde se consideran pesos elaborados en base a la naturaleza del negocio o a la importancia del riesgo, un método definitivamente más complejo.

En la figura 3.8 observamos una visión general sencilla de un método de auditoría basada en riesgos.

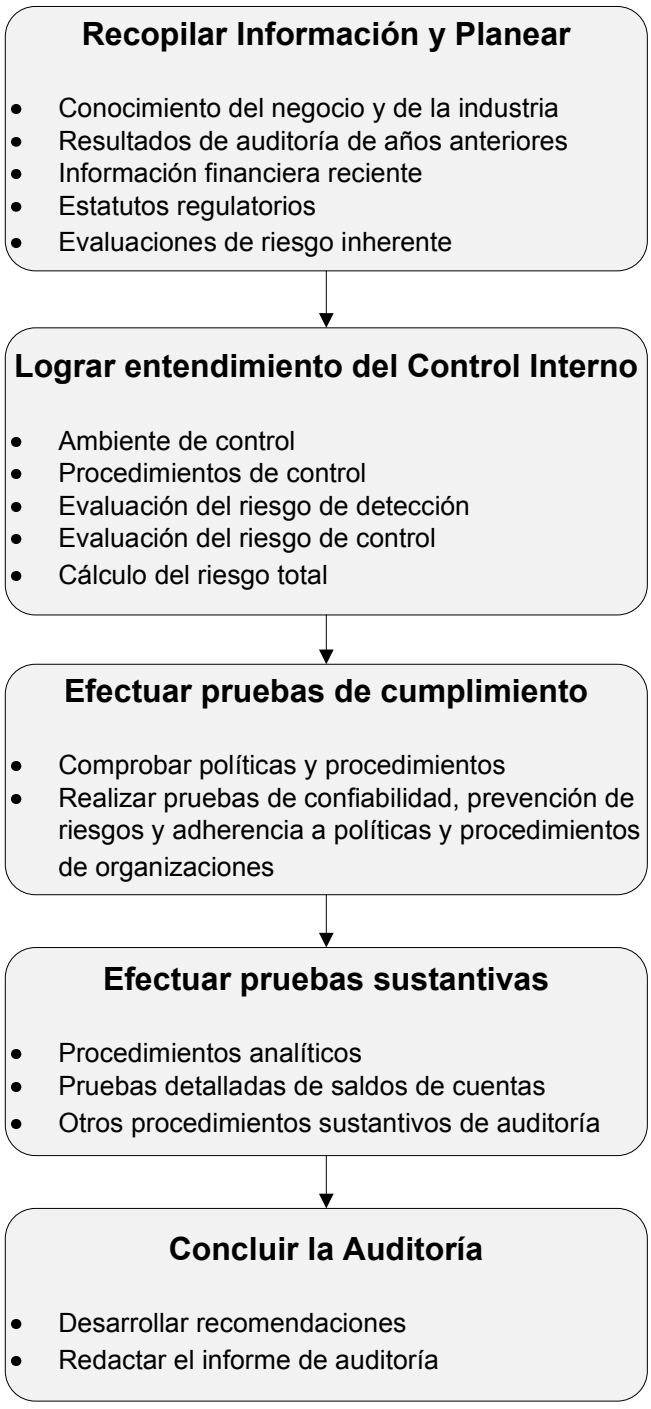

Figura 3.8 Enfoque de Auditoría Basado en Riesgos (ISACA, 2009)

CAPÍTULO 4

MODELAMIENTO DEL MANUAL DE AUDITORÍA INFORMÁTICA

4.1 El Problema

4.1.1 ¿Por qué se requiere una auditoría de sistemas?

La tecnología de información, soportada por recursos tales como información, infraestructura, aplicaciones y personas; se constituye en una herramienta estratégica que brinda rentabilidad y ventaja competitiva a las organizaciones frente a sus competidores en el mercado. Sin embargo, una mala administración de la tecnología deriva en riesgos que afectan negativamente a la empresa y sus operaciones.

De lo señalado, parte la siguiente interrogante: ¿cómo saber si estoy administrando de manera correcta la gestión tecnológica de mi organización?

La respuesta es mediante evaluaciones oportunas, especializadas e independientes a dicha función, sus procesos o los servicios que presta. En resumen, se requiere una auditoría de sistemas de información o auditoría informática, ejecutada por personal suficiente y competente y aplicando una metodología acorde a los requerimientos y necesidades de la organización.

Adicionalmente a lo señalado existen otras razones por las cuales se requiere de una auditoría informática, por ejemplo para certificar un servicio

tecnológico o por requerimiento regulatorio como es el caso de la COACS supervisadas por la SBS en el Ecuador.

El desarrollo de una auditoría se traduce en un proceso que aplicado adecuadamente permite a la administración de una organización el contar con una seguridad razonable de que las debilidades más importantes han sido identificadas, y que las mismas han sido o serán controladas en base a las recomendaciones desarrolladas como parte de la auditoría.

Es por tanto muy importante para el profesional en auditoría y particularmente para el auditor de sistemas de información el definir de forma precisa aspectos tales como, las unidades a auditar, el alcance, objetivos, aplicaciones, riesgos, controles a probar y las pruebas correspondientes. Todo esto con el fin de emitir una opinión que permita cumplir con su misión de evaluador y utilizar de forma eficiente los recursos de auditoría interna.

En base a lo mencionado surgen dos interrogantes fundamentales como son:

- ¿De qué forma puedo escoger los procesos de TI a ser evaluados durante el año?
- ¿Cómo puedo definir los controles a revisar para cada auditoría individual?

Es claro que existen varias respuestas en cada caso, sin embargo, en el presente capítulo se ha desarrollado una propuesta que busca brindar una referencia para ejecutar las tareas antes mencionadas de una manera sencilla y efectiva.

4.2 Proceso de Auditoría Propuesto

Conforme a lo mencionado anteriormente se definirán los procesos enfocados en la planificación anual de auditoría y la planificación de las auditorías individuales enfocados a una unidad de auditoría interna.

4.2.1 Proceso para la Planeación Anual de Auditoría

Como parte de las funciones de Auditoría Interna de las COACs, se requiere generar una planificación anual que permita administrar los recursos de auditoría y particularmente de la auditoria informática, distribuyéndolos en las diferentes revisiones que se realizarán durante el año. El mencionado plan debe ser desarrollado en base a una evaluación de riesgos de la Cooperativa, de esta forma se estará enfocando los esfuerzos de auditoría hacia lo que realmente le afecta a la institución en relación a la gestión tecnológica.

El auditor de sistemas de información debe conocer el proceso de evaluación de riesgos y las normas de auditoría relacionadas con el fin de liderar el proceso de planeación anual de auditoría de tecnología de información.

A continuación se muestran las actividades del proceso propuesto para la planeación anual de auditoría informática para COACs (figura 4.1):

Figura. 4.1 Proceso de Planeación Anual de Auditoría Informática

4.2.1.1 Comprender Objetivos y Procesos

Para que los auditores internos puedan agregar valor y mejorar el desempeño de la empresa, primero deben comprender su modelo de negocio.

El modelo de negocio incluye los objetivos de la empresa y la forma en que los procesos de negocio se estructuran para lograr estos objetivos.

Abarca la visión, la misión y los valores, así como también el conjunto de límites de la empresa, es decir, qué productos o servicios entregará, a qué clientes o mercados apuntará y qué canales de suministro y entrega utilizará.

Si bien el modelo incluye las estrategias y la dirección táctica sobre cómo la empresa realizará su implementación, también en él se incluyen las metas anuales que establecen los pasos específicos que la empresa adoptará al año siguiente y las medidas correspondientes al logro esperado.

4.2.1.2 Identificar Objetivos y Riesgos

Una vez que se tiene identificados los objetivos de negocio y los procesos clave correspondientes se procede a la identificación de los riesgos que podrían impedir el logro de los objetivos.

La capacidad de comprensión de los riesgos de negocio de parte del auditor interno es fundamental y determinará el grado en que se podrá agregar valor a la organización a través de los trabajos de auditoría interna.

Para cumplir con esta actividad se debe establecer una matriz de Objetivos y Riesgos

4.2.1.3 Evaluación de Riesgos

La evaluación de riesgos se debe hacer considerando y validando lo generado por el área de gestión de riesgos si esta existe y dependiendo de su nivel de madurez, el auditor deberá complementar en la medida de lo necesario la evaluación de riesgos para fines de su plan de auditoría

4.2.1.4 Análisis de Proceso y Riesgo

Una vez evaluados los riesgos se debe asociarlos a los procesos respectivos, la idea es identificar la vinculación existente entre un riesgo y aquellos procesos que lo originan.

Como resultado del análisis antes mencionado se obtiene la matriz de proceso y riesgo que se constituye en el punto de partida para realizar el plan de auditoría informática basado en riesgos.

4.2.1.5 Definición del Plan

Para definir el plan de auditoría se considera:

- El análisis de vinculaciones entre procesos y riesgos.
- La aplicación del enfoque de factor de riesgo.
- Se puede aplicar luego de los aspectos antes mencionados una clasificación de los procesos que serían sujetos de auditoría.
- Finalmente la definición de los procesos a ser auditados y los ciclos de auditoría respectivos comprenden el eje del Plan de Auditoría, posteriormente se debe realizar la estimación y asignación de recursos necesarios para la ejecución del plan.

- Los planes de auditoría basados en riesgos deberían ser actualizados anualmente pues es el período en que usualmente se actualiza la gestión de riesgos.

4.2.2 Proceso para una Asignación Individual de Auditoría

Para la definición del proceso aplicable a una asignación individual de auditoría se ha tomado como referencia las etapas del proceso de auditoría con enfoque a riesgos propuesto por ISACA.

El mencionado proceso se observa en la figura 4.2, a continuación:

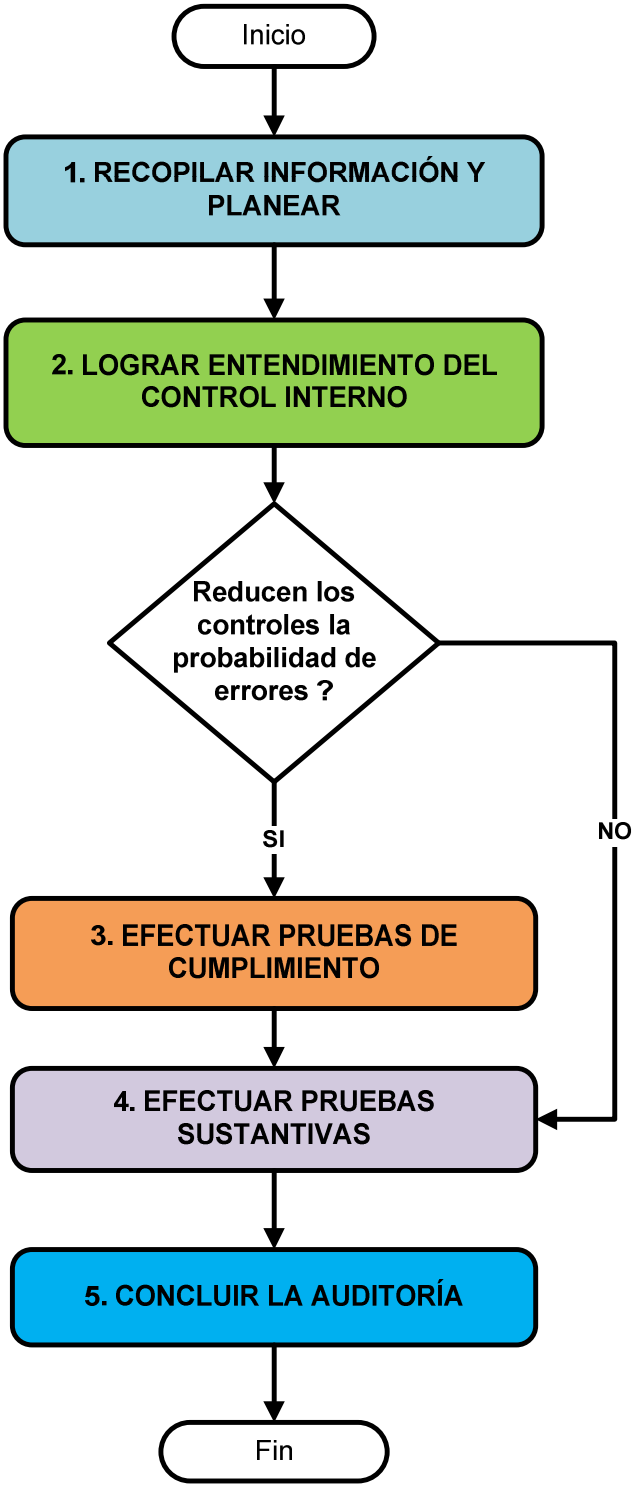

Figura 4.2 Proceso de Auditoría Informática con Enfoque a Riesgos

4.2.2.1 Recopilar Información y Planear

Este subproceso tiene como objetivo obtener el conocimiento de la historia y tipo de negocio de la Cooperativa dueña del(os) proceso(s) tecnológico(s) a ser auditado(s).

Dichas objetivos se consiguen en base a la ejecución de actividades tales como: revisión de resultados de auditorías de años anteriores, observación de información financiera reciente, revisión de las leyes y marco regulatorio aplicable a la institución.

Como resultado de este proceso se obtendrá como productos la definición del nivel de riesgo de auditoría y la evaluación de riesgo inherente. En esta etapa tomaremos en cuenta la metodología Magerit para la evaluación de los riesgos de tecnología de información.

4.2.2.2 Lograr Entendimiento del Control Interno

Esta etapa se enfoca en comprender el funcionamiento del sistema de control interno de la Cooperativa en lo relacionado al proceso objeto de la revisión. Esta evaluación permite al auditor conocer como la organización administra el control sobre sus procesos y actividades.

Las actividades que ayudan a cumplir con esta etapa son las siguientes: revisión de políticas y directrices relacionadas, aplicación de cuestionarios de control interno, identificar los procedimientos de control, evaluar el riesgo de control, evaluar el riesgo de detección, entre otros.

Como productos de esta etapa debemos contar con la valoración inicial de los riesgos de control y de detección.

4.2.2.3 Efectuar Pruebas de Cumplimiento

Una vez que el auditor tiene un conocimiento de las estructuras de control interno y ha identificado los controles asociados al proceso auditado, es necesario determinar si dichos controles reducen en forma significativa la probabilidad que se generen errores y riesgos en el desarrollo del proceso. En caso que los controles y su diseño cumplan con el objetivo de reducir el riesgo se deben realizar las pruebas de cumplimiento de dichos controles. Esta actividad permitirá conocer si los controles se ejecutan correctamente y si es posible depositar confianza sobre ellos.

Si por el contrario, el auditor identifica que los controles identificados muestran debilidades en su diseño y/o aplicabilidad se requiere ir directamente al siguiente paso del proceso, es decir aplicar las pruebas sustantivas o de detalle.

Las principales tareas a ejecutar como pruebas de cumplimiento incluyen la comprobación de políticas y procedimientos y realizar pruebas de confiabilidad y prevención de riesgos.

Esta actividad da como resultado la obtención de una valoración real del riesgo de control que permitirá realizar un análisis para identificar aquellos controles sobre los que el auditor deposita confianza (control adecuado) y aquellos sobre los cuales se requiere una revisión más profunda debido a las desviaciones en su cumplimiento.

4.2.2.4 Efectuar Pruebas Sustantivas

En esta etapa se busca definir de forma efectiva la integridad de transacciones individuales, datos u otra información. Es necesario realizar estas pruebas para conocer el estado de vulnerabilidad de un proceso que presenta ausencia o debilidad en su estructura de control.

Las pruebas sustantivas incluyen la ejecución procedimientos analíticos, pruebas detalladas de datos, recálculos y otros procedimientos detallados.

Como resultado de esta actividad se obtiene una evaluación del riesgo de detección obtenido para el proceso.

4.2.2.5 Concluir la Auditoría

Este subproceso busca presentar los resultados de la revisión realizada, el auditor se basa en el resultado de las pruebas ejecutadas para detectar debilidades de control y posibles riesgos que lo llevan a emitir una opinión formal y documentada del proceso o unidad auditable en estudio.

Dentro de las actividades principales a desarrollarse como parte de esta etapa caben la documentación de hallazgos, elaboración de recomendaciones y la redacción del producto final, es decir el informe de auditoría.

4.3 Manual de Auditoría Informática

4.3.1 Estructura

Una vez que se han definido los procesos principales a ser cubiertos en el manual de auditoría informática para COACs, se propone la siguiente estructura para el documento definitivo:

- Capítulo I “Introducción”: Antecedentes, marcos de referencia utilizados y beneficio para el auditor de sistemas.
- Capítulo II “Acerca del Manual”: Objetivos, estructura, enfoque y consideraciones de discrecionalidad técnica.
- Capítulo III “Planeación Anual de Auditoría”: Marco general en el cual se desarrollará la planeación anual de auditoría interna y los procedimientos asociados.
- Capítulo IV “Revisión Individual de Auditoría”: Marco general en cual se desarrollará la auditoría a una unidad auditable y los procedimientos respectivos.
- Capítulo V “Estándares de los papeles de trabajo”: Pautas y referencias para organizar los papeles de trabajo.
- Capítulo VI “Glosario”: Glosario de términos para ayuda del auditor de sistemas para entender las definiciones incluidas en el manual.
- Anexos: Documentos de trabajo y formatos utilizados por los procedimientos del manual.

El manual de auditoría informática para COACs, desarrollado en base al esquema anteriormente descrito, se encuentra en el Anexo No 4.1 del presente proyecto. .

CAPÍTULO 5

APLICACIÓN DEL MANUAL DE AUDITORÍA INFORMÁTICA

5.1 El Caso de la Cooperativa Internacional

A manera de ejemplo, el presente capítulo analiza el caso de una Cooperativa de Ahorro y Crédito, la cual requiere una auditoría de sistemas por parte del nuevo personal de auditoría informática recientemente contratado.

El ejemplo pretende ser ilustrativo, sin que el lector deba inferir conclusiones de estricto cumplimiento. Es claro que para riesgos, controles y situaciones similares pueden existir diferentes respuestas tanto por parte del auditor así como por los administradores de cada organización.

El texto utilizado para describir los eventuales hechos y situaciones del ejemplo se ha redactado en un lenguaje simple, como usualmente le llegaría al equipo de auditoría de sistemas luego de las entrevistas y averiguaciones pertinentes. El desarrollo del presente caso, permitirá llevar la descripción de la realidad hacia la terminología formal y técnica adoptada por la metodología propuesta en el manual de auditoría informática para COACs (desarrollado en el capítulo 3 de este proyecto).

5.1.1 La Historia

La Cooperativa Internacional, es una institución financiera con 40 años de experiencia en el negocio de la intermediación financiera del Ecuador. Fue formada por un grupo constituido por personas de la ciudad de Quito,

miembros de las asociaciones gremiales de profesores, policías y militares. Actualmente, la COAC Internacional tiene 200.000 socios, cuarenta sucursales en todo el Ecuador y cuenta con 500 empleados en su nómina.

Los servicios de la Cooperativa se enfocan principalmente en brindar crédito, administrar operaciones a plazo fijo y permitir el pago de luz, agua y teléfono en su red de oficinas.

La COAC se encuentra bajo el control de la SBS desde el año 2002, se halla dirigida por el Consejo de Administración constituido por cinco vocales que representan al organismo con mayor poder de decisión dentro de la institución, esto es la asamblea de representantes. Dicha asamblea ratifico al Gerente General y al Auditor Interno en la última sesión celebrada hace dos meses.

La Cooperativa, consciente de los nuevos cambios en el ambiente financiero y el creciente apoyo gubernamental hacia las instituciones de economía popular y solidaria; ha definido ingresar agresivamente en el campo de las transacciones por internet, banca electrónica y servicios web. A pesar del entusiasmo demostrado por la línea directiva (Consejo de Administración), existe recelo por parte del organismo de control interno representado por el Consejo de Vigilancia. Este hecho corresponde a que dicho comité conoce los fraudes asociados a transacciones en internet y la consiguiente afectación que ha representado para la imagen de la banca ecuatoriana.

Se ha solicitado al Auditor Interno la implementación de evaluaciones permanentes acerca de la gestión tecnológica de la Cooperativa, concentrando

su análisis en los aspectos que se consideran más importantes para la institución.

5.1.2 Estructura de la Cooperativa

La Cooperativa se encuentra formada por varias áreas entre las cuales se encuentran las siguientes:

1. Operaciones: enfocada en la gestión en agencias o sucursales
2. Crédito: cuya misión es controlar y gestionar la venta de crédito a nivel nacional
3. Finanzas: responsable de controlar las operaciones a plazo fijo, los procesos contables y los análisis de riesgo
4. Sistemas: encargado de mantener los servicios informáticos disponibles para los usuarios internos y externos.
5. Legal: cuya responsabilidad constituye la gestión del cobro de los créditos otorgados por la Cooperativa.
6. Recursos Humanos: responsable de la nómina y del sistema documental de la institución.
7. Riesgos: cuya responsabilidad se concentra en realizar evaluaciones enfocadas principalmente al riesgo de crédito, liquidez y operativo.
8. Auditoría Interna: encargada de evaluar y asesorar a la institución en temas de control interno, riesgo y fraude

El área de Sistemas es liderada por su Vicepresidente y agrupa a tres departamentos:

a. Departamento de Desarrollo de Aplicaciones: encargado de realizar los cambios sobre el sistema informático
b. Departamento de Producción, responsable de administrar los servicios tecnológicos y mantener las aplicaciones en producción
c. Departamento de Infraestructura, cuya función está enfocada en la red de datos (lan y wan), el hardware, instalaciones eléctricas y centro de cómputo.

5.1.3 Aplicaciones e Infraestructura

La COAC Internacional cuenta con los siguientes sistemas y herramientas informáticas:

- Sistema transaccional SISTRA que maneja las operaciones de préstamos, inversiones, los retiros/depósitos y la contabilidad, este aplicativo es desarrollado internamente y es modificado por parte de los programadores del departamento de desarrollo en base a las necesidades del negocio.
- Un sistema para el manejo de cajeros automáticos que se conecta con la red de ATMs a nivel nacional y realiza la comunicación con el sistema transaccional de la Cooperativa.
- Intranet Corporativa: utilizada para manejar el sistema documental de la Cooperativa, mediante esta herramienta el personal se mantiene informado de los reglamentos, manuales, procedimientos e instructivos que rigen la operación de la institución.

- Servicio de Correo electrónico, disponible para todo el personal con salida interna y externa y sin límite para transmisión de datos.
- Scoring de Crédito: Se trata de un aplicativo usado para evaluar las solicitudes de crédito que llegan a la institución. El sistema evalúa la información provista por el usuario y genera una calificación de riesgo que es crítica para el proceso de otorgamiento del crédito.
- Buró de Crédito, se trata de un aplicativo provisto por un tercero, el mismo que permite revisar al personal de la Cooperativa consultar información histórica del comportamiento crediticio del cliente.
- Mensajería instantánea mediante Messenger
- Internet disponible para cada computador de la red

En relación a infraestructura se cuenta con los siguientes elementos principales:

- Computadores personales para los empleados de matriz y sucursales, únicamente el personal de jefaturas y gerencias cuenta con equipos portátiles. Existen equipos que son de uso generalizado para ciertas ocasiones cuando los usuarios requieren movilizarse, son solicitados por los usuarios y facilitados por el departamento de infraestructura.
- La red de datos cuenta con un firewall implementado y funcionando
- Servidor de base de datos para almacenar la información para el sistema transaccional
- Servidor de correo implementado sobre linux

- Servidor web para publicar el sitio de la intranet
- Servidor virtual que almacena el aplicativo de ATMs
- Servidor proxy virtual para distribuir el internet
- Servidor de antivirus

5.2 Aplicación del Manual

Con base en la información anotada anteriormente, a continuación desarrollaremos los procesos de auditoría informática, tomaremos como referencia lo definido en el Manual de Auditoría Informática aplicado a Cooperativas de Ahorro y Crédito.

5.2.1 Definir el Plan Anual de Auditoría

Basados en las necesidades expresadas en la descripción del caso de estudio, el Auditor Interno solicita a su vez al Auditor de Sistemas Tecnológicos la elaboración del Plan de Anual de Auditoría Informática. Dicho documento, una vez revisado será puesto en consideración del Consejo de Vigilancia, para su aprobación formal.

Cabe indicar que el plan anual aprobado deberá ser ejecutado a lo largo del año con el fin de cumplir con los requisitos de eficiencia y oportunidad requeridos por la Cooperativa, adicionalmente, al ser parte del Plan Anual de Auditoría Interna, se encuentra sujeto a revisión por parte de los entes de control respectivos.

5.2.1.1 Comprender los Objetivos del Negocio

En esta fase, se realizó una reunión con la participación de los directores de todas las áreas de la Cooperativa en donde se explicaron los objetivos del trabajo a realizarse con el fin de levantar la información necesaria para elaborar el Plan Anual de Auditoría Informática. Se busca lograr el compromiso de los funcionarios con el trabajo de auditoría.

Se revisó el plan estratégico de la Cooperativa, obteniendo el conocimiento de la misión, visión y objetivos estratégicos de la Cooperativa. Es importante señalar que la planificación estratégica considera cinco años para su aplicación por tanto es muy útil para realizar una planificación a mediano y largo plazo. Los objetivos de la Cooperativa (estratégicos, operativos, de reportes financieros y cumplimiento regulatorio) se hallan enfocados a mejorar la rentabilidad de la institución mediante el aumento de su participación en el mercado a través de una mejor colocación de crédito, mayor captación de recursos mediante el producto inversiones a plazo fijo y conseguir una mayor cantidad de clientes. Así también el cumplimiento de las nuevas regulaciones gubernamentales es un aspecto importante para la institución.

A continuación se revisaron los documentos del Plan Operativo Anual (POA) el mismo que le permitió al auditor informático conocer las acciones, planes y proyectos que se realizaran durante el año en curso con el fin de cumplir con los objetivos estratégicos de la COAC. De este análisis se observó que la Cooperativa planea dar un gran énfasis a las transacciones electrónicas (banca electrónica, banca celular, pago de servicios por internet, atm, entre otros).

Mediante la revisión del mapa de procesos se logró observar las interacciones entre los procesos principales y su importancia para la Cooperativa. Se ratifica que los procesos de gestión de crédito, gestión de captaciones y gestión de servicios conexos (pagos, cobros, transferencias, entre otros) se constituyen en clave para el desarrollo de las operaciones de la Cooperativa.

Se realizaron entrevistas a los responsables de las áreas más comprometidas con el cumplimiento de los objetivos estratégicos (Operaciones, Crédito y Finanzas), esto con el fin de conocer los aplicativos o sistemas más importantes para el desarrollo de los procesos críticos y específicamente su relación con el cumplimiento de los objetivos institucionales.

Los resultados de esta etapa se registraron en el formulario PA-1 Lista de Objetivos de Negocio y Aplicativos Principales. (Ver anexo 5.1)

5.2.1.2 Identificar Objetivos y Riesgos de TI

En esta fase realizamos la definición de los objetivos y riesgos, dado que nuestro enfoque se basa en la gestión tecnológica debemos identificar los objetivos de la función de Tecnología de información derivados de los objetivos institucionales. Esta consideración se basa en lo especificado en el marco de buenas prácticas Cobit 4.1, el mismo que señala lo siguiente: "la estrategia de la empresa se debe traducir por parte del negocio en objetivos relacionados con iniciativas habilitadas por TI (las metas de negocio para TI)".

Dado que la Cooperativa no cuenta con objetivos específicos para tecnología de información, se procede a su desarrollo en base a la información de objetivos institucionales y aplicativos principales. Se genera la matriz respectiva en la cual se ha colocado las características de funcionamiento de cada aplicativo requeridas por el negocio para la consecución de cada objetivo institucional. El siguiente paso es redactar el objetivo basado en las aplicaciones y las condiciones requeridas de funcionamiento. A continuación se detalla un ejemplo relacionado al sistema SISTRA:

Sistema: SISTRA

Características de Funcionamiento:

- Seguridad (confidencialidad, integridad, disponibilidad)
- Desempeño
- Rapidez
- Adaptabilidad

Objetivos de TI:

a. Mantener el sistema SISTRA operando de forma segura y cumpliendo con los requerimientos de desempeño establecidos
b. Garantizar que el sistema SISTRA se adapta a los requerimientos del negocio y los entes de control

En base al análisis realizado en esta fase se obtiene como resultado los siguientes formatos:

- PA-2A Relación Entre Objetivos y Aplicativos Principales -

Características Solicitadas (Ver anexo 5.2)

- PA-2B Lista de Objetivos de TI (Ver anexo 5.3)
- PA-2C Lista de Objetivos de Negocio y Objetivos Ti (Ver anexo 5.4)
- PA-2D Riesgos Originados por Amenazas Tecnológicas (Ver anexo 5.5)

5.2.1.3 Evaluación de Riesgos

Durante esta fase, el auditor de sistemas requiere conocer si existe una relación entre las amenazas determinadas en el catálogo de MAGERIT y los objetivos de TI (definidos en la fase de identificación de objetivos). Para la identificación de dicha relación se desarrolló una matriz, la cual fue generada tomando en cuenta lo siguiente:

- En el eje vertical de la matriz se colocaron los objetivos de TI.
- En el eje horizontal de la matriz se incluyeron las amenazas especificadas en el catálogo de Magerit. Se seleccionaron las amenazas de tipo errores y ataques. Se mantuvo la codificación del catálogo, la misma que se conforma de una letra (“E” para errores y “A” para amenazas) más un número secuencial, de esta forma tenemos por ejemplo el error E1 o la amenaza A7.
- Se analizó la relación entre amenazas y objetivos respondiendo la siguiente pregunta: ¿la explotación de la amenaza afectaría el logro del objetivo?, en caso de ser afirmativo se coloca una marca (X) en el casillero correspondiente al objetivo y amenaza. Para nuestro caso particular se definió que las amenazas: “E1 - Errores de los

usuarios” y “A7 - Uso no previsto”, no se encuentran relacionadas con ningún objetivo de TI por lo cual quedan al margen del análisis. El resto de amenazas continúan a la siguiente actividad de esta etapa que es la determinación del riesgo residual. En la figura 5.1 se muestra el esquema de la matriz desarrollada.

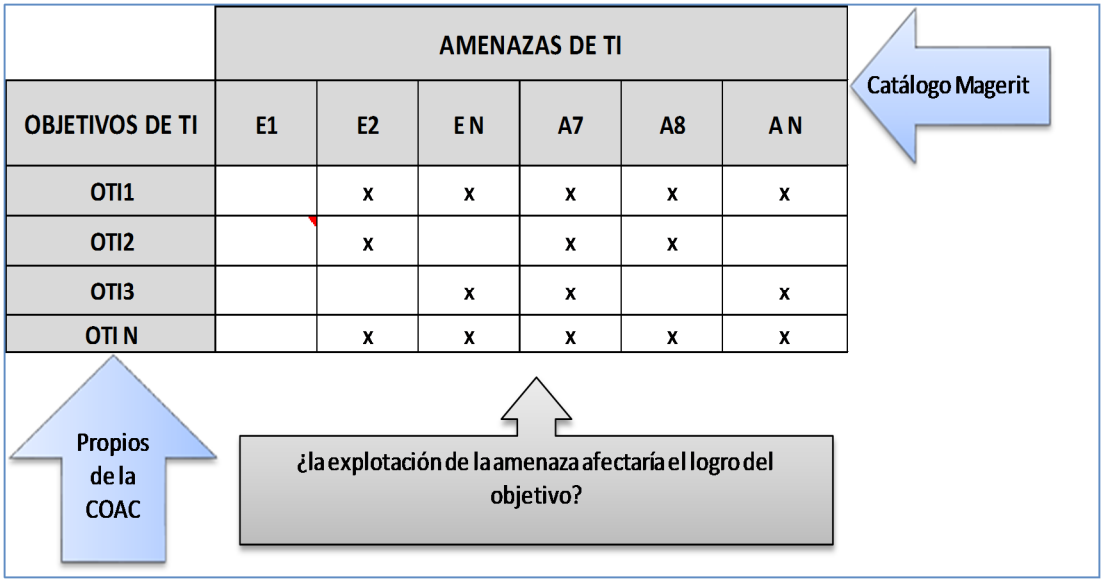

Figura 5.1 Matriz de Amenazas y Objetivos TI

En este punto, es necesario para el auditor de sistemas revisar información que le permita prepararse para valorar el impacto y la probabilidad de ocurrencia de las amenazas que afectan a los objetivos de TI de la Cooperativa. Por tal motivo es útil tener acceso a información de las evaluaciones de riesgo realizadas durante los dos años anteriores, concentrándose en los aspectos tecnológicos que puedan ser relevantes.

A continuación, el auditor de sistemas procede a desarrollar la evaluación de los riesgos propiamente dicha. En este punto se inicia estableciendo la escala que utilizaremos para valorar cualitativamente el impacto, la probabilidad de ocurrencia y el nivel de control asociado a cada amenaza. Esta valoración nos permitirá establecer los niveles de riesgo inherente y residual como función de dichas dimensiones. En la figura 5.2 se puede observar las dimensiones del riesgo.

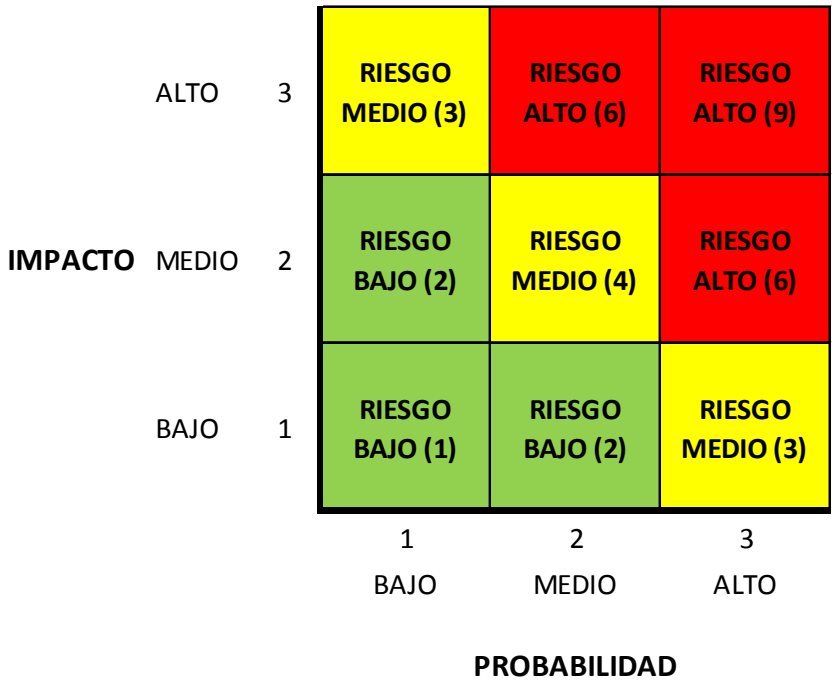

Figura 5.2 Dimensiones del Riesgo

Con el fin de valorar el impacto, la probabilidad de ocurrencia y el nivel de control asociado a cada amenaza, se definió utilizar tres niveles (alto, medio y bajo) a los cuales se les asigna una puntuación que luego permitirá efectuar el cálculo de riesgo inherente y residual. La definición de niveles se muestra en la tabla 5.1.

NIVEL DE IMPACTO PROBABILIDAD Y CONTROL	
ALTO	3
MEDIO	2
BAJO	1

Tabla 5.1 Niveles para valoración de impacto, probabilidad y control

En la siguiente actividad establecemos el valor del riesgo inherente o potencial, para esto se definen los valores de impacto y probabilidad de cada amenaza tomando como premisa un ambiente en ausencia de controles que puedan contrarrestar los efectos de dichos riesgos. El nivel de riesgo inherente se calcula en base al producto del impacto por la probabilidad de ocurrencia de la amenaza.

Para calificar el nivel de riesgo ya sea inherente o residual se utilizó la siguiente escala:

ESCALA PARA NIVEL DE RIESGO		
NIVEL	**MIN**	**MAX**
ALTO	6	9
MEDIO	3	5
BAJO	1	2

Tabla 5.2 Escala para definir el nivel de riesgo

De la calificación realizada se estableció que todas las amenazas mostraban un nivel de riesgo inherente alto o medio. (Ver tabla 5.2. Definición de Riesgo Inherente)

RIESGOS DE TI		IMPACTO	PROBABILIDAD	EXPOSICIÓN (IMPACTO X PROBABILIDAD)	NIVEL DE RIESGO INHERENTE - RI
E2	**Errores del administrador**	3	2	6	ALTO
E3	**Errores de monitorización (log)**	3	2	6	ALTO
E4	**Errores de configuración**	3	1	3	MEDIO
E9	**Errores de re encaminamiento**	2	2	4	MEDIO
E10	**Errores de secuencia**	3	1	3	MEDIO
E24	**Caída del sistema por agotamiento de recursos**	3	2	6	ALTO
A4	**Manipulación de la configuración**	3	1	3	MEDIO
A5	**Suplantación de la identidad del usuario**	3	3	9	ALTO
A9	**Re encaminamiento de mensajes**	3	1	3	MEDIO
A6	**Abuso de privilegios de acceso**	2	2	4	MEDIO
A10	**Alteración de secuencia**	3	2	6	ALTO
A11	**Acceso no autorizado**	3	2	6	ALTO
A13	**Repudio**	3	3	9	ALTO

Tabla 5.3. Definición de Riesgo Inherente

Lo que sigue, es la definición de los valores de controles o contramedidas (llamadas también salvaguardas) implementadas por la organización para enfrentar el riesgo. Estos valores respetan la escala descrita en la tabla 5.1. El nivel de control tiene una relación inversa al nivel de impacto o probabilidad del riesgo, mientras más alto es el nivel de control, significa que el riesgo se reduce, como resultado de la disminución del impacto o la probabilidad de ocurrencia de la amenaza. En la práctica, una vez valorado el nivel de control, se resta del valor del impacto o la probabilidad de ocurrencia (depende del tipo de control) y se vuelve a recalcular el riesgo, el mismo que ahora se denomina riesgo residual.

El resultado de la valoración de riesgo residual para el ejemplo se detalla en la tabla 5.4.

RIESGOS DE TI		IMPACTO	PROBABILIDAD	NIVEL DE CONTROL - NC	RIESGO RESIDUAL - RR	NIVEL DE RIESGO RESIDUAL
E2	Errores del administrador	3	2	2	2	BAJO
E3	Errores de monitorización (log)	3	2	1	4	MEDIO
E4	Errores de configuración	3	1	1	2	BAJO
E9	Errores de re encaminamiento	2	2	1	2	BAJO
E10	Errores de secuencia	3	1	1	2	BAJO
E24	Caída del sistema por agotamiento de recursos	3	2	1	4	MEDIO
A4	Manipulación de la configuración	3	1	2	1	BAJO
A5	Suplantación de la identidad del usuario	3	3	1	6	ALTO
A9	Re encaminamiento de mensajes	3	1	1	2	BAJO
A6	Abuso de privilegios de acceso	2	2	1	2	BAJO
A10	Alteración de secuencia	3	2	1	4	MEDIO
A11	Acceso no autorizado	3	2	1	4	MEDIO
A13	Repudio	3	3	1	6	ALTO

Tabla 5.4 Valoración de Riesgo Residual

Posteriormente el auditor de sistemas comunica los resultados al Auditor Interno o su delegado, en base al análisis conjunto se establece que existe una mayor preocupación por tratar los riesgos que alcanzaron un nivel de riesgo residual medio y alto. A esto se denomina el apetito de riesgo.

Con esta instrucción se seleccionaron aquellas amenazas que cumplen con esta condición especificada para el apetito de riesgo y que podemos apreciar en la tabla 5.5

RIESGOS DE TI		NIVEL DE RIESGO RESIDUAL
E3	**Errores de monitorización (log)**	MEDIO
E24	**Caída del sistema por agotamiento de recursos**	MEDIO
A5	**Suplantación de la identidad del usuario**	ALTO
A10	**Alteración de secuencia**	MEDIO
A11	**Acceso no autorizado**	MEDIO
A13	**Repudio**	ALTO

Tabla 5.5 Riesgos Seleccionados

El detalle de los resultados de esta etapa se encuentra documentado en los siguientes formatos:

- PA-3A Matriz de Objetivos de TI y Riesgos de TI (Ver anexo 5.6)
- PA-3B Matriz de Evaluación de Riesgos de TI (Ver anexo 5.7)

5.2.1.4 Análisis de Proceso y Riesgo

En esta etapa se seleccionaron los procesos de TI que requieren mayor atención por parte del auditor y por tanto son la base para efectuar la planificación del trabajo de auditoría informática.

Se tomaron los 34 procesos definidos por Cobit 4.1 y se confrontaron con las amenazas con riesgo residual de nivel alto y medio (definido en la

etapa de evaluación de riesgos). Se establecieron las relaciones en base a la consideración de aquellos procesos que podían dar origen a las amenazas identificadas. El establecimiento de las relaciones respondió en gran medida al juicio profesional del auditor de TI, cabe indicar que el dominio del marco de buenas prácticas Cobit 4.1 es indispensable para realizar dicha tarea. Adicionalmente, se utilizó como apoyo las relaciones entre procesos y criterios de información mencionados en el anexo II de Cobit 4.1. En este caso se definieron aquellos criterios de la información que serían afectados por la materialización del riesgo y luego se identificó cuáles eran los procesos que Cobit relaciona con dichos criterios. De esta forma se procedió a evaluar si dicha relación corresponde a la realidad de la Cooperativa. Como se mencionó anteriormente este mecanismo constituye una referencia para avanzar con el análisis de proceso y riesgo pero siempre dependerá del juicio profesional y conocimiento de la empresa por parte del auditor de sistemas o el equipo a cargo.

Los resultados de esta etapa se pueden observar en la tabla 5.6

		RIESGOS DE TI (Magerit)						
		E3	E24	A5	A10	A11	A13	
PROCESOS DE TI (Cobit 4.1)		Errores de monitorización (log)	Caída del sistema por agotamiento de recursos	Suplantación de la identidad del usuario	Alteración de secuencia	Acceso no autorizado	Repudio	TOTAL RIESGO PROCESO
PO1	Definir un Plan Estratégico de TI							0
PO2	Definir la Arquitectura de la Información	X		X	X	X	X	5
PO3	Determinar la Dirección Tecnológica							0
PO4	Definir los Procesos, Organización y Relaciones de TI							0
PO5	Administrar la Inversión en TI							0
PO6	Comunicar las Aspiraciones y la Dirección de la Gerencia							0
PO7	Administrar Recursos Humanos de TI							0
PO8	Administrar la Calidad	X						1
PO9	Evaluar y Administrar los Riesgos de TI	X	X	X	X	X	X	6
PO10	Administrar Proyectos							0
AI1	Identificar soluciones automatizadas							0
AI2	Adquirir y mantener software aplicativo	X					X	2

		RIESGOS DE TI (Magerit)						
		E3	E24	A5	A10	A11	A13	
PROCESOS DE TI (Cobit 4.1)		Errores de monitorización (log)	Caída del sistema por agotamiento de recursos	Suplantación de la identidad del usuario	Alteración de secuencia	Acceso no autorizado	Repudio	TOTAL RIESGO PROCESO
AI3	Adquirir y mantener infraestructura tecnológica		X				X	2
AI4	Facilitar la operación y el uso	X					X	2
AI5	Adquirir recursos de TI							0
AI6	Administrar cambios	X	X		X		X	4
AI7	Instalar y acreditar soluciones y cambios						X	1
DS1	Definir y administrar los niveles de servicio							0
DS2	Administrar los servicios de terceros			X		X	X	3
DS3	Administrar el desempeño y la capacidad							0
DS4	Garantizar la continuidad del servicio		X					1
DS5	Garantizar la seguridad de los sistemas	X	X	X	X	X	X	6
DS6	Identificar y asignar costos							0
DS7	Educar y entrenar a los usuarios							0
DS8	Administrar la mesa de servicio y los incidentes							0

		RIESGOS DE TI (Magerit)						
		E3	E24	A5	A10	A11	A13	
PROCESOS DE TI (Cobit 4.1)		Errores de monitorización (log)	Caída del sistema por agotamiento de recursos	Suplantación de la identidad del usuario	Alteración de secuencia	Acceso no autorizado	Repudio	TOTAL RIESGO PROCESO
DS9	Administrar la configuración		X					1
DS10	Administrar los problemas		X					1
DS11	Administrar los datos	X			X		X	3
DS12	Administrar el ambiente físico	X	X		X		X	4
DS13	Administrar las operaciones						X	1
ME1	Monitorear y Evaluar el Desempeño de TI						X	1
ME2	Monitorear y Evaluar el Control Interno						X	1
ME3	Garantizar el Cumplimiento Regulatorio	X	X	X	X	X		5
ME4	Proporcionar Gobierno de TI						X	1

Tabla 5.6 Matriz de Proceso/Riesgo

Como podemos observar en la columna "Total Riesgo Proceso", existen procesos que se relacionan con un mayor número de riesgos identificados, de esta forma es lógico dirigir la revisión de auditoría hacia dichos procesos con el fin de evaluar y proponer acciones para reducir los riesgos tecnológicos de la Cooperativa.

El detalle de los resultados de esta fase se muestra en el formato PA-4 Matriz de Proceso/Riesgo (Ver anexo 5.8).

5.2.1.5 Definición del Plan

Se tomaron los procesos con un nivel total de riesgo mayor a cero, se ordenaron de mayor a menor y se definieron en base a la tabla 5.7 los ciclos de revisión recomendados para cada uno de ellos. Esto quiere decir la frecuencia que el auditor de sistemas recomienda que ser audite cada proceso.

TOTAL RIESGO PROCESO		**CICLO DE REVISIÓN RECOMENDADO**
DESDE	**HASTA**	
5	6	Cada año
3	4	Cada dos años
1	2	Cada tres años

Tabla 5.7 Ciclos de Revisión de Procesos

En base a lo expuesto anteriormente el Plan de Auditoría queda de la siguiente forma:

CÓDIGO	PROCESOS DE TI	TOTAL RIESGO PROCESO	CICLO DE REVISIÓN
PO9	**Evaluar y Administrar los Riesgos de TI**	6	Cada año
DS5	**Garantizar la seguridad de los sistemas**	6	Cada año
PO2	**Definir la Arquitectura de la Información**	5	Cada año
ME3	**Garantizar el Cumplimiento Regulatorio**	5	Cada año
AI6	**Administrar cambios**	4	Cada dos años
DS12	**Administrar el ambiente físico**	4	Cada dos años
DS2	**Administrar los servicios de terceros**	3	Cada dos años
DS11	**Administrar los datos**	3	Cada dos años
AI2	**Adquirir y mantener software aplicativo**	2	Cada tres años
AI3	**Adquirir y mantener infraestructura tecnológica**	2	Cada tres años
AI4	**Facilitar la operación y el uso**	2	Cada tres años
PO8	**Administrar la Calidad**	1	Cada tres años
AI7	**Instalar y acreditar soluciones y cambios**	1	Cada tres años
DS4	**Garantizar la continuidad del servicio**	1	Cada tres años
DS9	**Administrar la configuración**	1	Cada tres años
DS10	**Administrar los problemas**	1	Cada tres años
DS13	**Administrar las operaciones**	1	Cada tres años
ME1	**Monitorear y Evaluar el Desempeño de TI**	1	Cada tres años
ME2	**Monitorear y Evaluar el Control Interno**	1	Cada tres años
ME4	**Proporcionar Gobierno de TI**	1	Cada tres años

12 Tabla 5.8 Ciclos Definidos de Revisión de los Procesos de TI

Cabe indicar que la planificación desarrollada debe ser ajustada en base a la realidad de cada organización (COAC), esto en relación a los recursos (humanos, equipos, software, logística, entre otros) y el presupuesto con el que cuente la institución para atender temas de Auditoría Informática.

El detalle de los resultados de esta etapa se encuentra en el formato denominado PA-5 Ciclos de Auditoría de los Procesos de TI (Ver anexo 5.9).

5.2.2 Revisión Individual de Auditoría

Continuando con la definición del caso de la Cooperativa Internacional, habíamos establecido el orden de revisión de los procesos de Cobit en base a lo detallado en la planificación anual (Ver tabla 5.8). De esta forma, se ha definido realizar la primera revisión de Auditoría Informática tomando como unidad auditable al proceso DS5: Garantizar la seguridad de los sistemas.

A continuación se detallan los objetivos y el alcance definidos por el Auditor Interno de la Cooperativa para la revisión de Auditoría Informática del mencionado proceso:

Objetivos:

- Evaluar las actividades desarrolladas por la Cooperativa para mantener la confidencialidad, integridad y disponibilidad de la información administrada por los aplicativos de la institución.
- Evaluar los controles asociados al proceso, estableciendo la opinión sobre el diseño, efectividad y el cumplimiento de los mismos.
- Evaluar los procesos implementados para la administración de incidentes de seguridad.
- Evaluar los niveles de riesgo del proceso y recomendar medidas para su adecuada administración.

Alcance:

Aplicativos principales de la Cooperativa y eventos generados entre el 01 de enero y el 30 de marzo del 2012.

5.2.2.1 Recopilar Información y Planear

Las actividades de esta fase inicial de la evaluación de auditoría informática consistieron en:

1. Se solicitó el manual de procedimientos de la Cooperativa, luego de su revisión se definió que la institución ha identificado sus procesos tecnológicos, sin embargo carecen de un procedimiento específico para seguridad de aplicaciones. Se cuenta con actividades que favorecen el aseguramiento de los sistemas pero las mismas se encuentran en los diferentes procedimientos de TI.
2. Se realizó entrevistas con personal de las gerencias de Negocios, Operaciones y Tecnología, con el fin de obtener su percepción de los controles implementados en las aplicaciones principales de la empresa.
3. Se realizó una visita al departamento de desarrollo, centro de cómputo y departamento de producción con el fin de conocer su interacción con el proceso de seguridad en las aplicaciones.
4. Anteriormente no se han realizado auditorías de seguridad de aplicaciones, por tanto no se cuenta con información histórica de debilidades detectadas en el pasado.

5. Se levantó un listado de los activos o recursos asociados al proceso en evaluación. Una vez identificados, los activos fueron valorados en base a su importancia para las actividades del proceso. Para el ejemplo, se trabajó con trece activos que fueron valorados frente a siete actividades definidas por Cobit 4.1 para el proceso “Garantizar la Seguridad de Aplicaciones”. Los resultados finales de la valoración de los activos se muestra en la tabla 5.9.

   Los activos se clasificaron en base a las cuatro categorías especificadas por Cobit 4.1, esto es: información, aplicaciones, personas e infraestructura.

ACTIVOS IDENTIFICADOS		**Valor total Activo**	
TIPO: APLICACIONES			
ACT1	Sistema Transaccional SISTRA	4	A
ACT2	Motor Transaccional ATM	3	M
ACT3	Intranet	2	B
ACT4	Banca Electrónica	3	M
ACT5	Correo Electrónico	3	M
ACT6	Scoring de Crédito	2	B
ACT7	Buro de Crédito	2	B
TIPO: PERSONAS			
ACT8	Personal de Desarrollo	2	B
ACT9	Personal de Producción	3	M
ACT10	Personal de Infraestructura	2	B
TIPO: INFRAESTRUCTURA			
ACT11	Red de datos	2	B
TIPO: INFORMACIÓN			
ACT12	Datos de gestión interna	3	M
ACT13	Datos de gestión externa	4	A

Tabla 5.9 Resumen de Valoración de Activos

6. Se realizó la evaluación del riesgo inherente del proceso, para esta tarea se tomó como referencia la metodología de análisis de

riesgos de Magerit versión 2.0, adaptándola a las necesidades de la auditoría. Las actividades desarrolladas en esta sub etapa se detallan a continuación:

- La evaluación inicia tomando en cuenta las amenazas especificadas en el catálogo de Magerit mismas que afectan a cada activo identificado. De esta forma se desarrolló una matriz por cada tipo de activo (información, aplicaciones, infraestructura y personas). La matriz se construyó en su eje vertical por el activo y su valor, mientras que en el eje horizontal constan las amenazas que afectan a todos los activos de la categoría.

  A continuación, se ingresó el valor para la degradación del activo en caso de materializase la amenaza respectiva, dicha degradación se expresa en niveles alto, medio o bajo. Tómese en cuenta que el análisis considera un ambiente sin controles.

  Se definió el valor de impacto en función del valor del activo y la degradación que la amenaza podría ocasionarle.
- A continuación, se ingresó el valor cualitativo correspondiente a la frecuencia de ocurrencia de la amenaza. Dicho valor corresponde a la escala definida en la tabla 5.8
- Finalmente se calcula el riesgo inherente como función del impacto calculado y la frecuencia de ocurrencia. De esta

forma tenemos definido el riesgo inherente de cada amenaza al materializarse sobre cada activo.

- Se procedió a generar la valoración de riesgo inherente por cada activo, cuyo resultado a la vez fue utilizado para definir el riesgo inherente por tipo de activos. Con esta información finalmente se estableció el nivel de riesgo inherente total del proceso. Cabe indicar que para el cálculo del riesgo total de un grupo de elementos se promediaron los valores de riesgo individual obtenido por cada elemento del grupo. En este caso el riesgo fue catalogado como MEDIO, tal como se muestra en la 5.10.

ACTIVOS - CATEGORIA	RIESGO INHERENTE	CATEGORÍA
INFORMACIÓN	3	MEDIO
APLICACIONES	4	ALTO
INFRAESTRUCTURA	3	MEDIO
PERSONAS	3	MEDIO
RIESGO TOTAL INHERENTE DEL PROCESO: GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS	3	MEDIO

Tabla 5.10 Calificación de Riesgo Inherente

Los resultados de esta etapa se encuentran documentados en los siguientes formatos:

- AI-1A Lista de Activos y Su Valor Para El Proceso (Ver anexo 5.10)
- AI-1B Lista de Amenazas Por Tipo de Activo (Ver anexo 5.11)
- AI-1C1 Evaluación de Riesgo Inherente - Componente: Información (Ver anexo 5.12)
- AI-1C2 Evaluación de Riesgo Inherente - Componente: Aplicaciones (Ver anexo 5.13)
- AI-1C3 Evaluación de Riesgo Inherente - Componente: Infraestructura (Ver anexo 5.14)
- AI-1C4 Evaluación de Riesgo Inherente - Componente: Personas (Ver anexo 5.15)
- AI-1C5 Evaluación de Riesgo Inherente – Valoración (Ver anexo 5.16)

5.2.2.2 Lograr Entendimiento del Control Interno

1. Tomando como referencia el marco de buenas prácticas Cobit 4.1 se seleccionaron los objetivos de control a revisar para definir el nivel de control interno del proceso.

   Para esto se definió una matriz con los objetivos de control especificados para el proceso DS5 Garantizar la seguridad en los sistemas, por parte de Cobit Quickstart, sin embargo el contenido de cada objetivo de control fue tomado directamente de Cobit 4.1 con el fin de darle un enfoque más detallado a la revisión.

   Posteriormente, se procedió a realizar una reunión con el Gerente de Sistemas con el fin de llenar la Matriz de Valoración de Control

Interno. De esta forma se asignaron los valores de riesgo de control asociado a cada objetivo, cabe indicar que un valor más alto representa un nivel de riesgo de control mayor o lo que es lo mismo un nivel de control insuficiente.

Luego de la valoración cualitativa realizada a cada objetivo se obtuvo el riesgo total de control el cual se determinó como ALTO (Ver tabla 5.11).

PUNTUACIÓN PROMEDIO	**4**
RIESGO DE CONTROL DEL PROCESO: GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS	**ALTO**

Tabla 5.11 Nivel de riesgo de control del proceso

2. Se estableció el riesgo de detección en base a lo definido en el manual de auditoría informática, se realizaron los cálculos considerando que el riesgo de auditoría se encuentra formado de los riesgos: inherente, de control y de detección. Dado que la fórmula a aplicar para el cálculo requiere valores expresados en porcentaje, se tomó como referencia la tabla 5.12 en donde se asigna los porcentajes a los diferentes niveles de riesgo identificado.

NIVEL	VALOR
MUY ALTO	70%
ALTO	60%
MEDIO	50%
BAJO	40%
MUY BAJO	30%

Tabla 5.12 Porcentaje de Riesgo por Nivel

Dado que es política del área de Auditoría Interna el mantener un valor de riesgo de auditoría no mayor al 5% para sus revisiones, se calculó el riesgo de detección, el mismo que se ubicó en 17% lo que equivale a muy bajo. A continuación (tabla 5.13) podemos observar los valores utilizados en el cálculo:

RIESGO	NIVEL	VALOR	COMENTARIO
RIESGO INHERENTE (RI)	MEDIO	50%	Valorado por el Auditor de Sistemas
RIESGO DE CONTROL (RC)	ALTO	60%	Valorado por el Auditor de Sistemas
RIESGO DE DETECCION (RD)	MUY BAJO	17%	Calculado RD = RA/(RI*RC)
RIESGO DE AUDITORIA	MUY BAJO	5%	Definido por la política de Auditoría Interna RA = RI x RC x RD

Tabla 5.13 Cálculo del riesgo de detección

Por lo descrito, se concluyó que el 70% de las pruebas deben ser de tipo sustantivas y el resto pruebas de cumplimiento, de esta forma se

podrá tener una mejor idea de las debilidades y riesgos del proceso a ser auditado.

3. Se realizó la planificación de las actividades de revisión mediante el desarrollo del programa de auditoría, basado en los objetivos, el alcance de la revisión y los niveles de riesgo identificados.

   Se tomaron como insumos los controles detallados en la matriz de valoración de riesgo de Control, los activos identificados con mayor riesgo inherente y también se consideró lo especificado en el documento de Cobit Assurance Guide que contiene una base muy completa de pruebas para cada objetivo de control de cada proceso detallado por Cobit 4.1.

Los resultados de las actividades de esta etapa de la auditoría se encuentran documentados en los siguientes formatos:

- AI-2A Matriz de Valoración de Riesgo de Control (Ver anexo 5.17)
- AI-2B Valoración del Riesgo de detección (Ver anexo 5.18)
- AI-2C Programa de Auditoría (Ver anexo 5.19)

5.2.2.3 Efectuar Pruebas de Cumplimiento

Para el desarrollo de las pruebas de cumplimiento se realizaron las siguientes tareas como medio para completar las actividades del programa de auditoría propuesto:

1. Se definió el tamaño de las muestras de usuarios, equipos, registros de incidentes de seguridad, roles de acceso a los sistemas SISTRA y Banca Electrónica.
2. En base al paso anterior se seleccionaron los casos de muestra para revisión
3. Se desarrollaron las actividades de revisión sobre la muestra, tales como verificación de documentación, entrevistas con el personal, observación de las instalaciones correspondientes a la red de datos, validación de las políticas de seguridad en los aplicativos, revisión informes de vulnerabilidades de la red de datos, revisión de la existencia de logs de seguridad en los aplicativos, verificación de formularios de acceso a los sistemas. Dichas actividades buscaron verificar el cumplimiento de los controles a fin de evaluar la efectividad de los mismos.
4. Luego de cada prueba se estableció el resultado de la misma y la confianza depositada en cada control, en el caso de los incumplimientos se levantaron los hallazgos con sus respectivas causas, el riesgo que representan y la recomendación para su tratamiento. Esta información se registró en la Matriz de objetivos de control y pruebas.
5. Se definieron los casos de controles que requirieron el desarrollo de pruebas sustantivas.

Los resultados de esta etapa se documentaron en el formato AI-3 Matriz de Objetivos de Control y Pruebas (Ver anexo 5.20)

5.2.2.4 Efectuar Pruebas Sustantivas

1. Se trabajó sobre los controles que requirieron pruebas sustantivas o de detalle, en este caso se ejecutaron actividades tales como:
    - Análisis de incidentes de seguridad registrados por la mesa de servicio.
    - Se realizó un hacking ético con el fin de identificar las vulnerabilidades de la red de datos.
    - Cruce de información entre el personal desvinculado de la Cooperativa y los accesos habilitados.
    - Prueba de captura de tráfico de red para verificar la encriptación de claves
    - Prueba de ingeniería social para verificar el sigilo de la clave de acceso al sistema transaccional SISTRA, entre otros.
2. Los resultados de esta fase fueron actualizados en la Matriz de objetivos de control y pruebas. Se informó directamente de una debilidad en la red de datos que permite el acceso al servidor de banca electrónica, esto debido a que la clave del firewall no había sido cambiada luego de su instalación. Los detalles de esta debilidad de riesgo crítico fueron informados utilizando el formato AI-4 Memorando de Hallazgo de Riesgo Crítico (Ver anexo 5.21).

5.2.2.5 Concluir la Auditoría

1. Tomando la información de los hallazgos registrados en la Matriz de objetivos de control y pruebas se procedió a redactar el borrador de informe final de auditoría informática referente al proceso en evaluación.
2. Se prepararon los papeles de trabajo y evidencias para soporte de cada hallazgo, por ejemplo se preparó un documento con la los resultados de la prueba de ingeniería social y las respuestas que cada persona entregó al auditor durante dicha prueba. Otro ejemplo es la gran cantidad de equipos con antivirus desactualizado, al respecto el papel de trabajo muestra un resumen de los computadores, los usuarios asignados y las áreas a las cuales pertenecen, la evidencia en cambio corresponde a pantallas del antivirus en la revisión in situ de cada computador.
3. El Auditor Interno en su papel de supervisor revisó el borrador de informe y sugirió dar un mayor énfasis a aquellas debilidades que podrían ser sujetas a la realización de fraudes ya sea internos como externos. En este punto se acordó dar una calificación de riesgo mayor a los hallazgos relacionados al sistema SISTRA y al servicio de banca electrónica.
4. La lectura del borrador de informe se realizó en presencia del Gerente General, el presidente del Consejo de Vigilancia, y los

directores de las áreas de Tecnología, Negocios, Operaciones y Recursos Humanos.

5. Se obtuvieron los compromisos por parte de responsables de cumplir las recomendaciones del informe y se registraron los planes de acción respectivos, los cuales fueron anexados al informe definitivo, el mismo que fue emitido formalmente por parte del Auditor Interno

El informe de auditoría generado como resultado de esta etapa se encuentra bajo el nombre de AI-4 Informe de Auditoría (Ver anexo 5.22).

CAPÍTULO 6

CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

1. La propuesta plasmada en el manual de auditoría informática para cooperativas de ahorro y crédito, provee una herramienta de referencia técnica y documental para la evaluación de los procesos de tecnología de dichas entidades financieras.
2. El uso de este manual está orientado hacia el personal de auditoría de sistemas que apoya a las unidades de auditoría interna de las Cooperativas de ahorro y crédito
3. La creciente automatización de los servicios financieros, ha posibilitado nuevas oportunidades de negocio para las cooperativas de ahorro y crédito, sin embargo esto también abre la posibilidad de nuevas amenazas para dichas entidades. Es por esto que el gobierno ha implementado nuevos mecanismos de control y supervisión enfocados hacia el componente tecnológico de dichas instituciones. Dichos mecanismos consideran a la auditoría informática como parte integrante en la evaluación del control interno y los riesgos de origen tecnológico.
4. La auditoría informática interna apoya los objetivos de la unidad de auditoría interna de las Cooperativas, evaluando el cumplimiento de la normativa establecida y asesorando a la alta dirección en temas orientados hacia la administración y control de los riesgos tecnológicos.

5. El marco de objetivos de control Cobit 4.1, permite al auditor de sistemas, soportar sus opiniones pues cuenta con un modelo de buenas prácticas aceptadas que proveen los objetivos de control a evaluados por el proceso de auditoría.
6. La metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT), se constituye en una referencia importante para cumplir con la auditoría de sistemas, específicamente en las tareas de análisis y evaluación de riesgos que apoyan la decisión de qué revisar y con qué nivel de detalle.
7. La auditoría informática interna, se desarrolla en base a dos procesos principales como son: la planificación anual, misma que se fundamenta en la planificación estratégica de la institución y las asignaciones individuales de auditoría que observan los riesgos y controles de los procesos de gestión tecnológica.
8. Es posible integrar la metodología de análisis y gestión de riesgos MAGERIT como parte del proceso de auditoría informática, seleccionando los componentes que apoyen al desarrollo de las actividades de evaluación tecnológica.
9. La inclusión de Cobit 4.1 en el proceso de auditoría de tecnología de información permite contar con un modelo de control que permite orientar los controles que se probarán con el fin de establecer una opinión del proceso evaluado.

10. Se ha desarrollado un caso de aplicación que si bien es un ejemplo, incluye varias situaciones reales obtenidas de la experiencia del autor del proyecto en varios años de trabajo como auditor informático en instituciones financieras. Las situaciones descritas permitieron la aplicación del manual de auditoría informática en su totalidad.
11. Las COACs están pasando por un periodo de transición en cuanto al tema normativo, sin embargo todavía se encuentran bajo el control de Superintendencia de Bancos y Seguros, por lo cual deben observar los requerimientos de la normativa de riesgo operativo y tecnológico mientras se completa dicha transición.
12. Varios de los pasos propuestos en el manual de auditoría son una guía para el auditor de sistemas, en varios puntos se confía en la experiencia, preparación y el criterio del profesional en auditoría de tecnología de información, así como de su conocimiento del giro del negocio, en este caso la intermediación financiera. También influye en gran medida el grado de conocimiento de la COAC a auditar, su procesos, servicios, tecnología y riesgos.
13. Es importante que las Coacs puedan ser auditadas en base a los riesgos propios de su realidad, esto permite un mejor uso de los recursos de auditoría que generalmente son limitados.
14. El uso de Cobit Quickstart para la selección de los objetivos de control de Cobit, constituye una herramienta valiosa que por su enfoque dirigido hacia organizaciones pequeñas o medianas, fácilmente se adapta a las

necesidad de la Cooperativas, eso si es necesario una evaluación previa la misma que nos permita clarificar su uso dentro de la auditoría.

15. Si bien la auditoría se enfoca en el cumplimiento legal y normativo, no es menos importante que su aporte es fundamental al momento de asesorar a la alta dirección en temas de control interno, es por eso que el presente trabajo incluye una relación muy estrecha con los objetivos institucionales, estratégicos y/o de negocio. Este enfoque procura que al aplicar el presente manual se busque apoyar el cumplimiento de los objetivos de la institución, identificando y administrando aquellas amenazas de tipo tecnológico.

6.2 Recomendaciones

1. Si bien el manual de auditoría informática enfoca los procesos de auditoría en base a sus actividades y entregables, se debe realizar un análisis adicional para su aplicación en cada Cooperativa, dicho análisis deberá considerar las particularidades de cada institución en materia de administración de negocio, tecnología, riesgos y auditoría.
2. La aplicación del manual de auditoría requiere que el lector cuente con un conocimiento previo de temas tales como: auditoría de tecnología de información, análisis de riesgos, control interno y el marco de buenas prácticas de Cobit 4.1. También es importante conocer la normativa legal para a las Coacs y tener una idea clara del funcionamiento de los servicios tecnológicos.

3. El importante tanto para las Cooperativas como para los entes de control respectivos, el promover acciones que permitan el desarrollo de las competencias del personal encargado de realizar el trabajo de auditoría informática interna. Esto con el fin de brindar un aporte que agregue valor a la institución financiera, así como evaluar el cumplimiento de la normativa legal aplicable a los procesos tecnológicos.
4. Los profesionales de la unidad de auditoría interna encargados de supervisar el trabajo de auditoría informática deben contar con la suficiente experticia para ejercer dicha función, el presente manual de auditoría informática les brinda una idea práctica de los procesos y actividades a supervisar.
5. El personal encargado de auditoría informática, debería considerar los objetivos de control de Cobit 4.1 como una referencia para realizar su trabajo. Sin embargo, para su aplicación es necesario considerar el tamaño, los servicios tecnológicos y el ambiente de control de la Cooperativa.
6. Con el fin de desarrollar la evaluación de riesgos respectiva, el personal de auditoría informática debe revisar la metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT) con el fin de obtener conocimiento respecto a los elementos básicos utilizados por el manual de auditoría informática propuesto.
7. El manual de auditoría informática debería ser usado para ejecutar los procesos principales del trabajo de auditoría de sistemas, sin embargo se debería complementar su uso mediante la consideración de otras

fuentes de información (normas de seguridad de información, gestión de servicios tecnológicos, continuidad del negocio, administración de proyectos, entre otras) que permitan actualizar los procesos y actividades definidas en el manual.

8. En el caso de la evaluación de los riesgos tecnológicos, se recomienda actualizar el análisis por lo menos una vez al año con el fin de incluir los cambios en los servicios de negocio, en la tecnología y en la normativa legal aplicable.
9. Con el fin de aplicar de manera efectiva el marco de buenas prácticas Cobit 4.1, considerado en los procesos de auditoría descritos en el manual, se recomienda considerar lo descrito en documentos tales como: Cobit Quickstart y Cobit IT Assurance Guide, que nos permiten enfocar la revisión de los controles y sus pruebas en base a las mejores prácticas de la industria descritas en dichos documentos complementarios.
10. Si bien la aplicación del presente proyecto se la realizó en base a plantillas desarrollada en hojas de trabajo de Excel, en ciertos tramos del proceso identificamos la necesidad de contar con una herramienta informática que permita automatizar el análisis de forma que se pueda obtener y comparar escenarios diferentes para la misma organización, proceso o activo. Es claro que el ciertos casos el análisis de riesgos puede tornarse muy extenso para el caso de organizaciones con gran cantidad de sistemas y objetivos de TI.

11. El presente manual sirve como una referencia para auditar Cooperativas de Ahorro y Crédito independientemente del esquema normativo que se encuentre vigente, es claro que el valor que agrega el trabajo de auditoría informática no es un tema meramente regulatorio sino de mejora del control interno sobre los procesos tecnológicos y el valor que entrega el área de tecnología hacia el negocio.
12. Considerar la aplicación de este manual en la unidades de auditoría interna de las COACs cuyos objetivos empresariales dependan en gran medida de servicios con alto componente tecnológico.
13. La valoración de riesgo puede ser realizada por varios medios, sin embargo se debe tener la suficiente experticia para equilibrar el aporte de dicha valoración frente el esfuerzo de realizarla, es fundamental conocer donde se encuentran las áreas críticas de la organización pero una análisis demasiado profundo puede agregar complejidad al trabajo de Auditoría. Esto sin mencionar que podría consumir recursos valiosos para el diseño, ejecución y valoración de pruebas.
14. Una vez, realizada la auditoría en base al manual especificado se puede incluir enfoques más específicos tales como: seguridad de la información, gestión de proyectos, continuidad del negocio, gestión de riesgos tecnológicos, entre otros; otorgando un nivel de mayor detalle y exigencia que promueva la mejora de la gestión tecnológica y la adopción de las mejores prácticas de la industria.

15. Es posible, desarrollar este modelo con un enfoque orientado hacia la Banca, es importante recordar que los marcos de buenas prácticas utilizados no son privativos de una sola industria o segmento productivo. Por tanto se podría adaptar los procesos tanto de planificación anual como de revisión individual para la ejecución de auditoría de sistemas en entidades bancarias. Es claro que se deberá considerar la integración de estructuras tales como; procesos de administración de riesgo tecnológico más desarrollados, aplicaciones con mayor número de clientes, sucursales o filiales en el exterior, portafolios de proyectos más grandes y complejos, programas de certificaciones, entre otros.

BIBLIOGRAFÍA

- Asamblea Nacional del Ecuador. (2008). *Constitución de la República del Ecuador.* Montecristi, Ecuador.
- Governance Institute. (2007). COBIT 4.1 *Control Objectives for Information and Related Technology – IT.* Illinois, EUA.
- Consejo Superior de Administración Electrónica. (2006). *MAGERIT versión 2 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Madrid, España.
- Isaca. (2009). *Manual de Preparación para el Examen CISA*. Illinois, EUA.
- Isaca. (2010). *Manual de Preparación al Examen CISA*. Illinois, EUA.
- Congreso Nacional. (2001). *Ley General de Instituciones del Sistema Financiero*. Quito, Ecuador.
- Presidencia de la República del Ecuador. (1994). *Reglamento a la Ley General de Instituciones del Sistema Financiero - Decreto Ejecutivo No. 1852. RO/ 475*. Quito, Ecuador.
- Asamblea Nacional del Ecuador. (abril del 2011). *Ley Orgánica de Economía Popular y Solidaria del Sistema Financiero*. Ecuador.
- Junta Bancaria. (2012). *Codificación de Resoluciones - SBS y Junta Bancaria.* Quito, Ecuador.
- Presidencia de la República del Ecuador. (2012). *Reglamento General de la Ley Orgánica de la Economía Popular y Solidaria del Sector Financiero Popular y Solidario*. Quito, Ecuador.

- Asociación Española de Normalización y Certificación. (2007). *Norma UNE-ISO/IEC 27001*. Madrid, España
- Asociación Española de Normalización y Certificación. (2009). *Norma UNE-ISO/IEC 27002*. Madrid, España
- Instituto Ecuatoriano de Normalización. (2009). *Norma NTE-ISO/IEC 27005*. Quito, Ecuador
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2004). *Gestión de Riesgos Corporativos. Marco Integrado*. Jersey City, EUA.
- Hernández Enrique. (2006). *Auditoría en Informática*. México DF, México: Compañía Editorial Continental.
- Dirección Nacional de Estudios e Información de la Superintendencia de Bancos y Seguros del Ecuador. (2012). *Comportamiento del Sistema de Cooperativas de Ahorro y Crédito a Marzo 2012*. Quito, Ecuador.
- Superintendencia de Bancos y Seguros del Ecuador. (2009). *Manual Único de Supervisión*. Quito, Ecuador.
- IT Governance Institute. (2007). *Cobit Quickstart Second Edition*. Illinois, EUA.
- Ernst and Young. (2002). *Preparación de Reportes Sobre Control Interno. Quito, Ecuador*.
- Coopers and Lybrand. (1997). *Los Nuevos Conceptos del Control Interno (Informe COSO)*. Jersey City, EUA.

- Badillo Jorge. (2011). *Módulo de Control Interno y Gestión de Riesgos – Método COSO*. Sangolquí, Ecuador.
- Rehage, K. & Hunt, S., (2008). *Developing the IT Audit Plan*. Florida, EUA: The Institute of Internal Auditors.
- IT Governance Institute. (2007). *IT Assurance Guide Using Cobit*. Illinois, EUA.
- Gutierrez García, N. (2009). *Las Cooperativas de Ahorro y Crédito en Ecuador y sus Transformaciones Durante los Últimos Diez Años*. (Tesis de maestría inédita). Facultad Latinoamericana de Ciencias Sociales - Sede Ecuador, Quito, Ecuador.
- Whittington, O. Ray. & Pany, Kurt. (2000). *Auditoría un Enfoque Integral*. Bogotá, Colombia: McGraw Hill
- Whittington, O. Ray. & Pany, Kurt. (2005). *Principios de Auditoría*. México DF, México: McGraw Hill

Internet:

- Centro Criptológico Nacional de España. (2012). *Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional de España*. Recuperado de: https://www.ccn-cert.cni.es
- Superintendencia de Bancos y Seguros del Ecuador. (2012). *Codificación Resoluciones SBS y Junta Bancaria.* Recuperado de: http://www.sbs.gob.ec/practg/sbs_index?vp_tip=12
- Asociación Nacional de Cooperativas de Ahorro y Crédito Controladas por la Superintendencia de Bancos y Seguros del Ecuador. (2012).

Las cooperativas en Ecuador. Recuperado de: http://www.ficoop.coop/index.php?option=com_content&view=article&id=14

- Poderes Inteligencia Política. (2012). *Cerca de 900 cooperativas pasarán en un año a la nueva superintendencia.* Recuperado de: http://poderes.com.ec/2012/cerca-de-900-cooperativas-pasaran-en-un-ano-a-la-nueva-superintendencia/
- Instituto Nacional de Economía Popular y Solidaria - IEPS - República del Ecuador. (2012). *Cooperativas a nivel nacional*. Recuperado de: http://www.ieps.gob.ec/web/index.php?option=com_content&view=article&layout=edit&id=378
- Risk Management Society. (2012). *What is ERM?* Recuperado de: http://www.rims.org/resources/erm/pages/WhatisERM.aspx
- Information Systems Audit and Control Association. (2012). COBIT 4.1: Framework for IT Governance and Control. Recuperado de:http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx
- Universidad del Cauca. (2013). *Normas Internacionales de Auditoría*. Cauca, Colombia. Recuperado de: http://fccea.unicauca.edu.co/old/evaluacion.htm

ABREVIATURAS Y ACRÓNIMOS

SIGLAS	SIGNIFICADO
ACSB	Asociación de Cooperativas Reguladas
CLUSA	Liga de Cooperativas de los Estados Unidos
COAC	Cooperativa de Ahorro y Crédito
COLAC	Confederación Latinoamericana de Cooperativas de Ahorro y Crédito
CUNA	Credit Union Nacional
FECOAC	Federación Nacional de Cooperativas de Ahorro y Crédito
INEN	Instituto Ecuatoriano de Normalización
ISO	Internacional Standard Organization
PDCA	Plan (planear). Do (hacer). Check (chequear) y Act (actuar)
SBS	Superintendencia de Bancos y Seguros
SWISSCONTACT	Fundación Suiza de Cooperación para el Desarrollo Técnico
WOCCU	Organización Mundial de Cooperativas de Ahorro y Crédito

ANEXOS

Anexo 4.1 Manual de Auditoría Informática.

Anexo 5.1 PA-1 Lista de Objetivos de Negocio y Aplicativos Principales

Anexo 5.2 PA-2A Relación Entre Objetivos y Aplicativos Principales - Características Solicitadas

Anexo 5.3 PA-2B Lista de Objetivos de TI

Anexo 5.4 PA-2C Lista de Objetivos de Negocio y Objetivos TI

Anexo 5.5 PA-2D Riesgos Originados por Amenazas Tecnológicas

Anexo 5.6 PA-3A Matriz de Objetivos de TI y Riesgos de TI

Anexo 5.7 PA-3B Matriz de Evaluación de Riesgos de TI

Anexo 5.8 PA-4 Matriz de Proceso/Riesgo

Anexo 5.9 PA-5 Ciclos de Auditoría de los Procesos de TI

Anexo 5.10 AI-1A Lista de Activos y Su Valor Para El Proceso

Anexo 5.11 AI-1B Lista de Amenazas Por Tipo de Activo

Anexo 5.12 AI-1C1 Evaluación de Riesgo Inherente - Componente: Información

Anexo 5.13 AI-1C2 Evaluación de Riesgo Inherente - Componente: Aplicaciones

Anexo 5.14 AI-1C3 Evaluación de Riesgo Inherente - Componente: Infraestructura

Anexo 5.15 AI-1C4 Evaluación de Riesgo Inherente - Componente: Personas

Anexo 5.16 AI-1C5 Evaluación de Riesgo Inherente – Valoración

Anexo 5.17 AI-2A Matriz de Valoración de Riesgo de Control

Anexo 5.18 AI-2B Valoración del Riesgo de detección

Anexo 5.19 AI-2C Programa de Auditoría

Anexo 5.20 AI-3 Matriz de Objetivos de Control y Pruebas

Anexo 5.21 AI-4 Memorando de Hallazgo de Riesgo Crítico

Anexo 5.22 AI-5 Informe de Auditoría