



UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

TÍTULO DEL TRABAJO DE INVESTIGACIÓN

**GUÍA DE IMPLEMENTACIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
APLICANDO COBIT EN AUDITORIAS DE ENTIDADES FINANCIERAS,
PARA DISMINUIR ERRORES PROCEDIMENTALES.**

AUTOR

Patricia Alexandra Badillo Pinto

AÑO 2015-2016

PÁGINA DE REVISIÓN

Los miembros del Tribunal de Graduación del proyecto de investigación de título: **GUÍA DE IMPLEMENTACIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN APLICANDO COBIT EN AUDITORIAS DE ENTIDADES FINANCIERAS, PARA DISMINUIR ERRORES PROCEDIMENTALES**, presentado por: **Sra. BADILLO PINTO PATRICIA ALEXANDRA**, y dirigida por: **Ing. FERNANDO MOLINA**.

Una vez escuchada la defensa oral y revisado el informe final del proyecto de investigación con fines de graduación escrito en la cual se ha constatado el cumplimiento de las observaciones realizadas, remite la presente para uso y custodia en la biblioteca de la Facultad de Ingeniería de la UNACH.

Para constancia de lo expuesto firman:

Ing. Danny Velasco
Presidente del Tribunal



Firma

Ing. Alejandra Pozo
Miembro del Tribunal



Firma

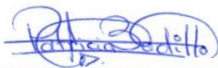
Ing. Fernando Molina
Miembro del Tribunal



Firma

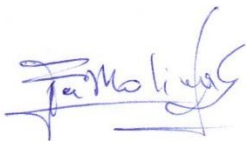
AUTORÍA DE LA INVESTIGACIÓN

La responsabilidad del contenido de este Proyecto de Graduación, corresponde exclusivamente a: BADILLO PINTO PATRICIA ALEXANDRA e ING. FERNANDO MOLINA GRANJA; y el patrimonio intelectual de la misma a la Universidad Nacional de Chimborazo.



Badillo Pinto Patricia Alexandra

C.I. 0603552654



Ing. Fernando Molina

C.I. 0602328072

AGRADECIMIENTO

Mi agradecimiento en primer lugar a Dios, por haberme dado valor y fuerza para culminar esta etapa profesional.

A su vez al Ing. Fernando Molina, por su apoyo al realizar el trabajo investigativo.

A mi familia que me han apoyado en todo el transcurso de mis estudios dándome apoyo y ánimos para culminar con esta etapa.

Gracias a todos quienes colaboraron con su conocimiento en este proyecto.

Patricia Alexandra Badillo Pinto

DEDICATORIA

Yo, Patricia Alexandra Badillo Pinto dedico esta investigación a Dios, a mi Hijo, a mis Padres, Hermanos y Amigos mismos que con su apoyo moral han influido para terminar esta etapa más de mi vida profesional.

Patricia Alexandra Badillo Pinto

TABLA DE CONTENIDO

Contenido

SUMMARY.....	¡Error! Marcador no definido.
INTRODUCCIÓN.....	1
CAPÍTULO I MARCO TEÓRICO	4
1.1 TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES.	4
1.2 AUDITORÍA	4
1.3 AUDITORÍA INFORMÁTICA.....	5
1.4 OBJETIVOS DE LA AUDITORÍA INFORMÁTICA.....	5
1.5 FUNCIONES DE LA AUDITORÍA INFORMÁTICA.....	5
1.6 TIPOS DE AUDITORÍA INFORMÁTICA	5
1.7 METODOLOGÍAS DE AUDITORÍA INFORMÁTICA.....	6
1.8 PRUEBAS Y HERRAMIENTAS USADAS PARA EFECTUAR UNA AUDITORÍA INFORMÁTICA.....	7
1.9 AUDITORÍA INFORMÁTICA EN INSTITUCIONES FINANCIERAS.	7
1.10 NORMAS Y PROCEDIMIENTOS PARA AUDITAR SISTEMAS INFORMÁTICOS	8
CAPÍTULO II ANÁLISIS SITUACIONAL DE LA COOPERATIVA DE AHORRO Y CRÉDITO NUEVA ESPERANZA.....	21
2.1 INTRODUCCIÓN	21
2.2 PROBLEMÁTICA	21
2.3 ANTECEDENTES	22
2.4 INFORMACIÓN DE LA INSTITUCIÓN	23
2.5 ESTRATEGIA	28
2.6 SEGURIDAD INFORMÁTICA.....	29
2.7 HIPÓTESIS.....	30
2.8 IDENTIFICACIÓN DE VARIABLES.....	30
CAPÍTULO III GUÍA DE IMPLEMENTACIÓN APLICANDO COBIT.....	32
3.1 GUÍA DE IMPLEMENTACIÓN	32
3.2 DEFINIR TAREAS Y RESPONSABLES.	32
3.3 IDENTIFICAR LOS PROCESOS DE LA COOPERATIVA QUE SE VAN A EVALUAR....	34
3.4 DEFINICIÓN DE DOMINIOS Y PROCESOS DE COBIT 5.	35
3.5 DEFINICIÓN DE DOMINIOS COBIT.	36

3.6	SELECCIÓN DE LOS PROCESOS DE COBIT ASOCIADOS A LOS PROCESOS DE LA COOPERATIVA.	36
3.7	METODOLOGÍA	42
CAPÍTULO IV EJECUCIÓN DE LA EVALUACIÓN Y ANÁLISIS DE RESULTADOS		46
4.1	PLANIFICACIÓN DE LA EVALUACIÓN	46
4.2	DIRECTRICES DE LA AUDITORÍA	46
4.3	MEDICIÓN DEL NIVEL DE MADUREZ DE LOS PROCESOS	47
4.4	EJECUCIÓN DE LA EVALUACIÓN	50
4.5	ANÁLISIS DE LOS RESULTADOS.....	84
4.6	COMPROBACIÓN DE LA HIPÓTESIS.....	91
CAPÍTULO V CONCLUSIONES Y RECOMENDACIONES		94
5.1	CONCLUSIONES	94
5.2	RECOMENDACIONES.....	96
GLOSARIO DE TÉRMINOS.....		97
BIBLIOGRAFÍA		99
ANEXOS.....		103

ÍNDICE DE TABLAS

Tabla 1 Grupo evaluador.	33
Tabla 2 Procesos de la Cooperativa de Ahorro y Crédito Nueva Esperanza asociados al marco de COBIT 5.	42
Tabla 3 Operacionalización de variables	44
Tabla 4 Tabla de procedimientos	45
Tabla 5 Directrices de auditoría de APO01.	50
Tabla 6 Directrices de auditoría de APO02.	52
Tabla 7 Directrices de auditoría de APO03.	53
Tabla 8 Directrices de auditoría de APO04.	55
Tabla 9 Directrices de auditoría de APO07.	59
Tabla 10 Directrices de auditoría de APO11.	60
Tabla 11 Directrices de auditoría de APO12.	63
Tabla 12 Directrices de auditoría de BAI02.	67
Tabla 13 Directrices de auditoría de BAI03.	69
Tabla 14 Directrices de auditoría de BAI05.	71
Tabla 15 Directrices de auditoría de DSS04.	75
Tabla 16 Gestionar servicios de seguridad de DSS05.	78
Tabla 17 Directrices de auditoría de MEA01.	81
Tabla 18 Directrices de auditoría de MEA02.	82
Tabla 19 Directrices de auditoría de MEA03.	83
Tabla 20 Análisis de indicadores.	92

ÍNDICE DE FIGURAS

Figura 1 Técnicas de auditoría.....	9
Figura 2 Principios del modelo COBIT.....	13
Figura 3 Usuarios.....	14
Figura 4 Recursos informáticos.....	16
Figura 5 Modelo de Madurez "Process Capability Model" de COBIT 5. ISACA. (2011).....	19
Figura 6 Niveles de capacidad y atributos de procesos. (Armenta Fonseca, 2014).....	20
Figura 7 Organigrama General de la Cooperativa. Manual de Perfiles (2012).....	27
Figura 8 Procesos de COBIT 5. (COBIT 5 (2012)).....	35
Figura 9 Niveles de Capacidad. (Orta Pedroza, 2014).....	47
Figura 10 Ejemplo del cálculo del proceso APO02.....	49
Figura 11 Análisis de indicadores.....	92
Figura 12 Comprobación de la hipótesis aplicando COBIT 5.....	93

RESUMEN

El principal objetivo del presente trabajo es desarrollar una guía de implementación del modelo COBIT en auditorías a instituciones financieras que será implementada específicamente en la Cooperativa de Ahorro y Crédito Nueva Esperanza. Para ello se ha estructurado el presente documento en cinco capítulos que abarcan el marco teórico, análisis situacional de la institución, desarrollo de la guía de implementación, ejecución de la evaluación y análisis de los resultados, y las respectivas conclusiones y recomendaciones.

El proyecto abarca la recopilación de datos referentes a la Institución y los principales procesos a evaluar. A estos se les aplica las directrices de COBIT que permiten verificar el cumplimiento de los procesos con el fin de emitir un resumen que muestre las falencias existentes.

Finalmente se realiza un análisis de los resultados obtenidos y se plantean recomendaciones para facilitar la toma de decisiones por parte de los directivos de la Institución, que permitirá establecer una cultura de seguridad en el manejo de la información en los procesos de negocio.



**UNIVERSIDAD NACIONAL DE CHIMBORAZO
FACULTAD DE INGENIERÍA
CENTRO DE IDIOMAS**



Lic. Karen Plua

10 de Marzo del 2016

SUMMARY

The main objective of this work is to develop a Model Implementation Guide COBIT is for Audits financial institutions to be implemented specifically in the Cooperative de ahorro y crédito Nueva Esperanza. This has been structured for this document in five chapters covering the theoretical framework, situational analysis Institution Development Implementation Guide, Running the Evaluation and Analysis of Results and respective conclusions and recommendations.

The project involves the collection of data on the institution and the main process to be evaluated these apply the guidelines them The COBIT they allow verifying compliance with the processes to the UN to issue summary shows the weaknesses.

Finally the UN Analysis of the results obtained and Recommendations Make arise to facilitate decision-making by the directors of the institution, which will establish a culture of safety in the handling of 'information Business Processes.



INTRODUCCIÓN

El uso de las tecnologías de la información cobra cada día mayor importancia y relevancia en los distintos sectores de la población. Uno de los sectores que mayor crecimiento ha tenido en el país es el sector financiero, el cual ha crecido tanto en usuarios como en agencias o unidades bancarias. Por lo que las entidades financieras no han quedado exentas del auge de las tecnologías de la información. (Aguilera, 2009).

Existen diferentes modelos para realizar las auditorías informáticas en las instituciones financieras, ejemplos de ellos podemos mencionar el sistema COSO y el COBIT.

Países como Estados Unidos y Colombia tienen estos sistemas establecidos para realizar sus auditorías informáticas a entidades financieras. En Ecuador, aunque se utilizan, aún no están normadas e implementadas para su ejecución, por lo que la confección de una guía de implementación del modelo COBIT en auditorías a instituciones financieras contribuirá a erradicar errores en su ejecución y por ende la aparición de datos erróneos o fuga de información. (Council, 2006).

PLANTEAMIENTO DEL PROBLEMA

Las entidades financieras son responsables del control de los bienes financieros de sus clientes. (Alcántara, 2009). La tecnología es el instrumento indicado para proporcionar un servicio de calidad y certificar que los procesos de control sean efectivos. (Abu-Masa, 2008).

Cada país escoge los modelos o sistemas por el cual se rigen para realizar las auditorías informáticas a entidades financieras. En Ecuador, aunque no está implementado de manera normativa, muchas de las empresas financieras utilizan las distintas variantes del Sistema COBIT, sin existir una guía de implementación para el mismo que permita su unificación de criterios a la hora de su aplicación. (Brito & Echavarría, 2009)

Uno de los problemas que se afrontan en la realización de auditorías informáticas a unidades financieras en el cantón Riobamba, las cuales permiten mantener un riguroso control interno de la información disponible, es que no existe implementada una metodología que rijan o norme los requisitos, pasos, esquemas y métodos para la aplicación de las tecnologías de la información con

el fin de realizar las auditorías informáticas, según nos reportan autores como Naranjo y Freire en sus estudios realizados en los años 2010 y 2011. (Naranjo, 2010), (Freire, 2011).

FORMULACIÓN DEL PROBLEMA

¿De qué manera pueden disminuir los errores procedimentales al aplicar una guía de implementación de las tecnologías de la información, aplicando COBIT, en auditorías a instituciones financieras?

OBJETIVOS OBJETIVO GENERAL

Desarrollar una guía de implementación de tecnologías de la información aplicando COBIT en auditorías de entidades financieras, para disminuir errores procedimentales.

OBJETIVOS ESPECÍFICOS

- Identificar marcos de referencia, metodologías y estándares internacionales del modelo COBIT.
- Identificar marcos de referencia, metodologías y estándares internacionales del modelo COBIT que se adapten a la realidad ecuatoriana.
- Identificar marcos de referencia, metodologías y estándares internacionales del modelo COBIT para auditorías en instituciones financieras que se adapten a la realidad ecuatoriana.
- Identificar los procesos y objetivos control de COBIT para auditorías en instituciones financieras, que pueden ser fortalecidos.
- Desarrollo de una guía metodológica de referencia.
- Validar guía metodológica de referencia, en la Cooperativa de Ahorro y Crédito Nueva Esperanza.

JUSTIFICACIÓN

El uso del modelo COBIT presupone un mejor control y una garantía para evitar la indebida manipulación de la información de usuarios de estas unidades financieras. (López & Soriano, 2012).

La confección de una guía de implementación de este modelo de auditoría, presupone un salto cualitativo en cuanto a calidad de los procesos de auditoría. Su aplicación permitirá optimizar el proceso de implementación del modelo COBIT en auditorías a instituciones financieras, llevando a la institución financiera hacia un nivel superior de seguridad, eficacia, control y satisfacción para sus clientes. (ISACA, 2010).

CAPÍTULO I MARCO TEÓRICO

1.1 TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES.

El término tecnologías de la información es usado con frecuencia para referirse a cualquier forma de hacer cómputo. Se necesita una base muy sólida de conocimientos relacionados con el estudio de los conceptos fundamentales de áreas como las ciencias de la computación, así como capacidad y habilidades de gestión del personal encargado para lograr planificar y gestionar la infraestructura de Tecnologías de la Información y las Comunicaciones (TICS) de una organización. De ahí que se considere que es un trabajo difícil y complejo. (Aguilera & Riascos, 2009).

De lo anterior se deriva que los profesionales de TICS asumen la responsabilidad de la selección de productos de hardware y software adecuados para una organización, a la vez que combinan correctamente los conocimientos, prácticas y experiencias para hacer frente a las necesidades y exigencias tanto la infraestructura de tecnología de información de una organización como de las personas que lo utilizan. (Castilla, 2006).

Otras de sus funciones son la de integrar los productos con las necesidades y la infraestructura organizativa, mediante la instalación, la adaptación y el mantenimiento de los sistemas de información, lo que garantiza proporcionar un entorno seguro y eficaz que apoya las actividades de los usuarios del sistema de una organización y eleva los niveles de satisfacción de los clientes con el servicio prestado.

1.2 AUDITORÍA

Es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas. (Piattini M. y Del Peso E. (2007)).

1.3 AUDITORÍA INFORMÁTICA

J.J. Acha define auditoría informática como “un conjunto de procedimientos y técnicas para evaluar y controlar total o parcialmente un sistema informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existente en cada empresa y para conseguir la eficacia exigida en el marco de la organización correspondiente”. (Piattini M. y Del Peso E. (2007)).

1.4 OBJETIVOS DE LA AUDITORÍA INFORMÁTICA

La auditoría informática (AI) confirma la consecución de los objetivos tradicionales de la auditoría: objetivos de protección de activos e integridad de datos; y objetivos de gestión, que abarcan no solamente los de protección de activos, sino también los de eficacia y eficiencia. (Piattini M. y Del Peso E. (2007))

1.5 FUNCIONES DE LA AUDITORÍA INFORMÁTICA

Dentro del proceso de auditoría es importante asegurar que se cumplan por lo menos los principios básicos de un proceso formal. Los elementos indispensables para cumplir este requisito son: la planeación, el control y el seguimiento del desempeño, que deberán garantizar lo siguiente:(Apuntes de Auditoría Informática, 2009).

- Que los recursos de informática sean orientados al logro de los objetivos y las estrategias de las organizaciones.
- La elaboración, difusión y cumplimiento de las políticas, controles y procedimientos inherentes a la AI.
- Que se den los resultados esperados por la institución mediante la coordinación y apoyo recíproco con: auditoría, asesores externos, informática, y la alta dirección.

1.6 TIPOS DE AUDITORÍA INFORMÁTICA

- **Auditoría de las bases de datos:** Controles de acceso, de actualización, de integridad y calidad de los datos.

- **Auditoría de la seguridad:** Referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.
- **Auditoría de la seguridad lógica:** Comprende los métodos de autenticación de los sistemas de información.
- **Auditoría de la seguridad en producción:** Errores, accidentes y fraudes. (Echenique J. y McGraw H. (2001)).

En el presente trabajo se considera necesario aplicar los dos primeros tipos de auditorías mencionados anteriormente debido a que una institución financiera debe garantizar la confidencialidad e integridad de los datos.

1.7 METODOLOGÍAS DE AUDITORÍA INFORMÁTICA

La metodología es necesaria para que un equipo de profesionales alcance un resultado homogéneo tal como si lo hiciera uno sólo. Por ello, resulta habitual el uso de metodologías en las empresas auditoras/consultoras profesionales (desarrolladas por los más expertos) para conseguir resultados similares (homogéneos) en equipos de trabajo diferentes (heterogéneos). (Piattini M. y Del Peso E. (2007))

Las metodologías que se puede encontrar en la auditoría informática son dos familias distintas (Piattini M. y Del Peso E. (2007))

Las auditorías de controles generales: Cuyo objetivo es dar una opinión sobre la fiabilidad de los datos del ordenador para la auditoría financiera. El resultado externo es un escueto informe como parte del informe de auditoría, donde se destacan las vulnerabilidades encontradas. Están basadas en pequeños cuestionarios estándares que dan como resultado informes muy generalistas.

Las metodologías de los auditores internos: Están formuladas por recomendaciones de plan de trabajo y de todo el proceso que se debe seguir, por tanto, están basadas en profesionales de gran nivel de experiencia y formación, capaces de dictar recomendaciones técnicas, operativas y jurídicas, que exigen una gran profesionalidad y formación. De la misma forma se describe en forma de cuestionarios genéricos, con una orientación de los controles a revisar. El auditor interno debe crear sus metodologías necesarias para auditar los distintos aspectos o áreas en el plan auditor.

1.8 PRUEBAS Y HERRAMIENTAS USADAS PARA EFECTUAR UNA AUDITORÍA INFORMÁTICA

Al elaborar una auditoría informática el auditor puede realizar las siguientes pruebas (Echenique J. y McGraw H. (2001)):

- Pruebas clásicas: Consiste en probar las aplicaciones/sistemas con datos de prueba, observando la entrada, la salida esperada, y la salida obtenida. Existen paquetes que permiten la realización de estas pruebas.

- Pruebas sustantivas: Aportan al auditor informático las suficientes evidencias y que se pueda formar un juicio. Se suelen obtener mediante observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones. Verifican así mismo la exactitud, integridad y validez de la información.

- Pruebas de cumplimiento: Determinan si un sistema de control interno funciona adecuadamente según la documentación, según declaran los auditados y según las políticas y procedimientos de la organización.

Las principales herramientas de las que dispone un auditor informático son:

- Observación
- Realización de cuestionarios
- Entrevistas a auditados y no auditados
- Flujogramas
- Listas de chequeo

1.9 AUDITORÍA INFORMÁTICA EN INSTITUCIONES FINANCIERAS.

Las entidades financieras manejan un importante cúmulo de información de sus clientes, por lo que están en riesgo en todo momento de que la misma sufra daños, ya sea por fugas o por mala manipulación, lo que causaría serios problemas a sus usuarios internos y externos. (Alcántara, 2009).

Las auditorías financieras se conceptualizan como el proceso de verificación y revisión de las manifestaciones hechas en los estados financieros y debe efectuarse de acuerdo con las normas de auditoría generalmente aceptadas, es un examen sobre la contabilidad y otros registros. Su principal función consiste en revisar la correcta y oportuna aplicación de los registros contables y operaciones financieras de las empresas, comprobar la emisión de los resultados financieros de un ejercicio fiscal y emitir un dictamen sobre los resultados. (Castellanos, 2007).

Una de las características de cualquier actividad auditora está relacionada con las funciones de control. Por ello la participación de la auditoría informática en el sector financiero la constituye la revisión de las aplicaciones informáticas con el objeto de asegurar que cumplan con los criterios funcionales y operativos definidos por la entidad financiera. Los sistemas de información de bancos y entidades financieras tienen entre sus características particulares la de construir fuentes de datos para múltiples agentes externos. La importancia de la auditoría informática debe garantizar el correcto funcionamiento de los sistemas, no solo desde la perspectiva de la gestión de la propia empresa sino también desde la óptica de los clientes.

La auditoría informática en las entidades financieras suele aportar con la detección de procesos obsoletos, ineficaces o redundantes, que no añaden valor a la actividad de negocio y que sin embargo suponen un coste. El auditor informático tiene la oportunidad de analizar la información, los procesos operativos relacionados con los productos y tratamientos informáticos. (Piattini M. y Del Peso E. (2007)).

1.10 NORMAS Y PROCEDIMIENTOS PARA AUDITAR SISTEMAS INFORMÁTICOS

La Auditoría de Sistemas de Información es un trabajo de naturaleza especializada y las habilidades necesarias para llevar a cabo este tipo de auditorías requieren el desarrollo y la promulgación de normas específicas para la práctica profesional como las emitidas por la Asociación de Auditoría y Control de Sistemas de Información (ISACA) las cuales son aplicables para el trabajo de auditoría realizado por miembros de la asociación y por las personas que han recibido la designación de Auditor Certificado de Sistemas de Información (CISA, por sus siglas en inglés), aunque a criterio personal pueden servir de base para cualquier auditor que cuente con

las habilidades y destrezas suficientes y necesite apoyarse en una normativa específica para realizar su trabajo, debido a que el planteamiento a nivel general es similar a la normativa para la realización del trabajo de cualquier auditoría por lo que en el presente trabajo se considera la más adecuadas para una auditoría de sistemas de información.

ISACA ha implementado **estándares** que definen los requerimientos obligatorios para la auditoría y para los informes de auditoría de sistemas informáticos, **directrices** que brindan una guía para aplicar los estándares de auditoría de sistemas informáticos y **procedimientos** que ofrecen ejemplos de procedimientos que debe seguir un auditor de sistemas informáticos en una asignación de auditoría de este tipo. Además se tienen en cuenta las normas internacionales que comprenden normas ético-morales y normas profesionales que todo auditor debe tener en cuenta durante el desarrollo de su auditoría.

Algunos de los estándares más conocidos que cumplen con estas normas y políticas son:

COBIT: Control Objectives for Information and related Technology. Desarrollado por Information Systems Audit and Control Association (ISACA). Centra su interés en la gobernabilidad, aseguramiento, control y auditoría para Tecnologías de la Información y Comunicación (TIC).

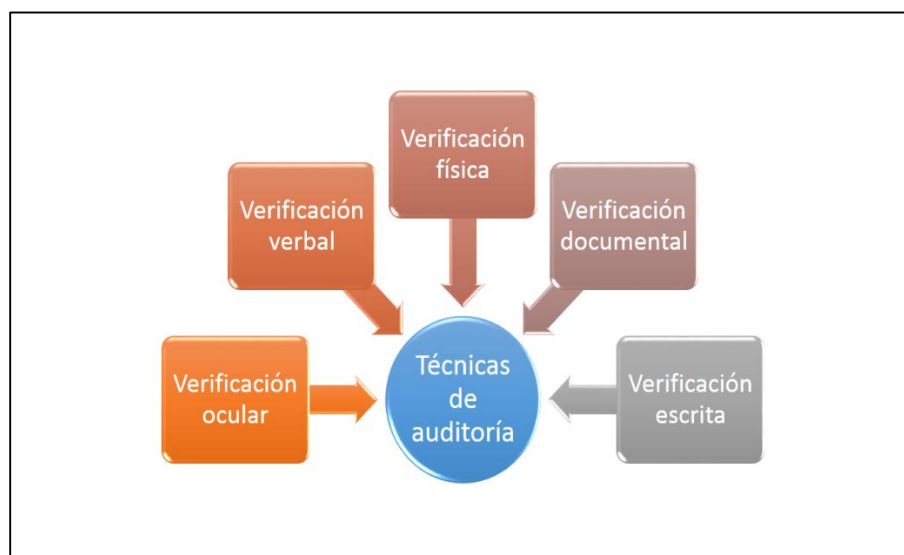


Figura 1 Técnicas de auditoría.

ITIL: Information Technology Infrastructure Library. Recoge las mejores prácticas para administrar los servicios de Tecnología de la Información (TI).

COSO: Committee of Sponsoring Organizations. Hace recomendaciones a los administradores de TI sobre cómo evaluar, informar e implementar sistemas de control, teniendo como objetivo la efectividad y eficiencia de las operaciones, la información financiera y el cumplimiento de las regulaciones, valoración de riesgos, actividades de control, información y comunicación y la verificación.

Brinda el enfoque de una estructura común para comprender al control interno, el cual puede ayudar a cualquier entidad a alcanzar logros en su desempeño y en su economía, prevenir pérdidas de recursos, asegurar la elaboración de informes financieros confiables, así como el cumplimiento de las leyes y regulaciones, tanto en entidades privadas, como en públicas.

COSO está enfocado a toda la organización, contempla políticas, procedimientos y estructuras organizativas además de procesos para definir el modelo de control interno. (Durán Jacobo, 2010).

SAC: Systems Auditability and Control, ofrece una guía de estándares y controles a auditores internos sobre la forma de controlar y auditar los sistemas de información y tecnología.

1.10.1 MODELO COBIT

Es un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso.

Las siglas COBIT significan Objetivos de Control para Tecnología de Información y Tecnologías relacionadas (Control Objectives for Information Systems and related Technology). El modelo es el resultado de una investigación con expertos de varios países, desarrollado por ISACA (Información Systems audit. and Control Association).

La estructura del modelo COBIT propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden

la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización.

La primera edición del COBIT, fue publicada en 1996 y fue vendida en 98 países de todo el mundo. La segunda edición, fue publicada en Abril de 1998, desarrolla y mejora lo que poseía la anterior mediante la incorporación de un mayor número de documentos de referencia fundamentales, nuevos y revisados objetivos de control de alto nivel, intensificando las líneas maestras de auditoría, introduciendo un conjunto de herramientas de implementación, así como un CD-ROM completamente organizado el cual contiene la totalidad de los contenidos de esta segunda edición. (Marco Quintanilla, 2015).

COBIT 5 fue creado para ayudar a las organizaciones a obtener el valor óptimo de TI manteniendo un balance entre la realización de beneficios, la utilización de recursos y los niveles de riesgo asumidos. COBIT 5 posibilita que TI sea gobernada y gestionada en forma holística para toda la organización, tomando en consideración el negocio y áreas funcionales de punta a punta así como los interesados internos y externos. Se puede aplicar a organizaciones de todos los tamaños, tanto en el sector privado, público o entidades sin fines de lucro. (Marco Quintanilla, 2015).

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

Una de las muchas características anticipadas de COBIT 5 es el incremento en la atención de la integración del negocio y TI. Esta orientación mejorará la comunicación, clarificará los roles y responsabilidades y reducirá los incidentes relacionados con la información y la tecnología que pudieran dañar a la organización.

COBIT 5 integra todas las mejores prácticas dispersas en los distintos marcos de referencia de ISACA – COBIT, VAL IT, Risk IT, BMIS (Modelo de negocios para la seguridad de la información) e ITAF (Marco de referencia para el aseguramiento de TI) en una sola base de conocimiento que permita tener un acercamiento consistente del valor, riesgo y seguridad en la

organización. La arquitectura de COBIT 5 junta a los interesados (stakeholders), sus preocupaciones, intereses y necesidades así como la base de conocimiento de ISACA. (ISACA. (2011).)

En esencia, COBIT 5 cubre de manera completa la organización y provee una base de integración de otros marcos de referencia, estándares y mejores prácticas que algunas organizaciones pueden ya estar usando, por lo que se ha decidido utilizar el COBIT 5 como modelo para auditar los principales procesos informáticos de la Cooperativa de Ahorro y Crédito Nueva Esperanza de la provincia de Chimborazo.

1.10.2 MODELO COBIT COMO MARCO DE REFERENCIA PARA LA AUDITORIA INFORMÁTICA.

El modelo COBIT intenta responder a las necesidades del negocio, siendo a la vez independiente de la plataforma técnica de TI adoptada en la organización. Su marco referencial visualiza la información necesaria para dar soporte a los procesos del negocio y la combina con los recursos tecnológicos los que deben ser administrados por los procesos de TICS, siendo su fuerte la combinación de los “requerimientos de negocio para la información” con los principios referenciales existentes. (Abu-Masa, 2008).

La misión de COBIT es el investigar, desarrollar, publicar y promover un conjunto de objetivos de control generalmente aceptados, autorizados, actualizados por ISACA para ser utilizadas en el día a día por la gerencia del negocio, los profesionales de IT y de la seguridad. En la figura 3 vemos que define también procesos, metas y métricas para el control. (IT Governance Institute, 2007).

Al establecer la lista de requerimientos, COBIT combina los principios contenidos en los modelos referenciales existentes y conocidos: requerimientos de Calidad que incluyen calidad, costo, entrega y distribución; requerimientos fiduciarios como son el cumplimiento de las leyes y regulaciones y requerimientos de Seguridad basados en confidencialidad, integridad y disponibilidad que lo hacen acreedor de credenciales útiles para la realización de auditorías en entidades financieras. (Council, 2006).

En este modelo se consideran los requerimientos de calidad dentro de su metodología con los criterios de integridad, efectividad, además compara a la calidad de entrega y servicio con la disponibilidad, siendo este el resultado del manejo apropiado del riesgo como resultado de la comparación de oportunidades, el costo es considerado por la eficiencia. (ISACA, 2010).

En COBIT 5 para la Seguridad de la Información, los principios de seguridad de la información comunican las reglas de la empresa que soportan los objetivos de gobierno y los valores empresariales, según la definición del Consejo y la dirección ejecutiva. Estos principios deben:

- Ser limitados en cuanto a su número.
- Estar expresados en un lenguaje sencillo y declarar, de la manera más clara posible, los valores fundamentales de la empresa. (COBIT Focus, 2014).

El modelo COBIT 5 se construye sobre cinco principios básicos, que quedan cubiertos en detalle e incluyen una guía exhaustiva sobre los catalizadores para el gobierno y la gestión de las TI de la empresa.



Figura 2 Principios del modelo COBIT.

COBIT 5 proporciona ventajas a gerentes, usuarios finales, auditores, responsables de TI y Organismos estatales de control.

Los gerentes se benefician de COBIT porque les provee un fundamento sobre el cual basar las decisiones. La toma de decisiones es más eficaz porque COBIT ayuda en la definición de un plan de TI estratégico, la definición de la arquitectura de la información, la adquisición del hardware necesario y el software para ejecutar una estrategia, la aseguración del servicio continuo, y la supervisión del funcionamiento del sistema TI. Los usuarios se benefician de COBIT debido al aseguramiento proporcionado a ellos en el tratamiento de la información. Los auditores o interventores se ven beneficiados porque COBIT permite identificar cuestiones de control de TI dentro de la infraestructura de una institución y a corroborar sus conclusiones de auditoría. Los responsables de TI, ya que pueden identificar los controles requeridos en cada una de sus áreas y finalmente los organismos de control para saber lo que pueden exigir.

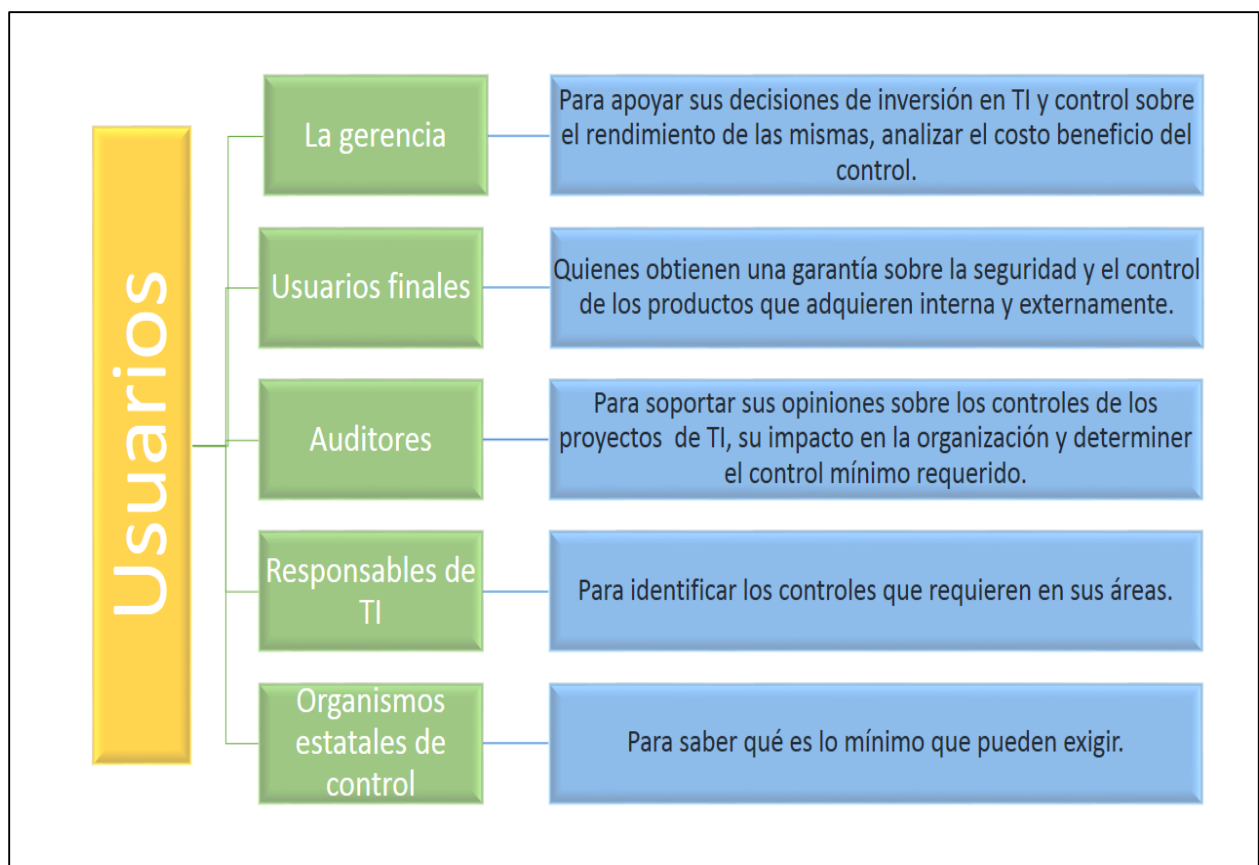


Figura 3 Usuarios

1.10.3 Estructura del marco referencial COBIT

El marco de referencia de COBIT consta de objetivos de control de TI de alto nivel y de una estructura general para su clasificación.

Considera que un elemento crítico para el éxito y la supervivencia de las organizaciones es la administración efectiva de la información y de la tecnología de información (TI) relacionada con ella. Debido a que en esta sociedad cada vez más globalizada, la información puede viajar a través del ciberespacio sin las restricciones de tiempo, distancia y velocidad, busca enfatizar este aspecto crítico en base a:

- La creciente dependencia en la información y en los sistemas que proporcionan esa información.
- La creciente vulnerabilidad y un amplio espectro de amenazas sobre la información.
- La escala y el costo de las inversiones actuales y futuras en tecnología de información.
- El potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos. (Dionicio Teo, 2011).

Por lo que en la actualidad muchas organizaciones pueden considerar a la información y la tecnología que la soporta, como sus más valiosos activos.

El ámbito empresarial se desarrolla mediante la competitividad y el dinamismo, propiciando que la gerencia generalmente incremente sus expectativas relacionadas con la entrega de servicios de tecnología de información. Ciertamente, la información y los sistemas de información pueden llegar a ser penetrantes en las organizaciones, desde las plataformas del usuario hasta las redes locales, estructuras cliente servidor y equipos mainframe. Derivado de esto, la administración requiere niveles de servicio que presenten incrementos de calidad, funcionalidad y facilidad de uso, así como un mejoramiento continuo y una disminución de los tiempos de entrega, al tiempo que demanda que esto se realice a un costo más bajo. (Dionicio Teo, 2011).

Muchas organizaciones reconocen los potenciales beneficios que puede proporcionarle la tecnología de información, sin embargo, si desean ser exitosas, también deben comprender y administrar los riesgos asociados con la implementación de nueva tecnología. Por lo tanto, la

administración debe tener una apreciación y un entendimiento básico de los riesgos y limitantes de la utilización de tecnología de información para proporcionarle una dirección efectiva y controles adecuados. COBIT ayuda a salvar la brecha existente entre riesgos de negocio, necesidades de control y aspectos técnicos al proporcionar las mejores prácticas a través de un marco de trabajo de dominios y procesos y presentar un detalle de actividades en una estructura manejable y lógica. Las mejores prácticas de COBIT representan el consenso de los expertos, ayudan a la administración a optimizar la inversión en tecnología de información, pero aún más importante, representan aquello sobre lo que serán evaluados al momento de surgir eventualidades importantes. (Dionicio Teo, 2011).

Las organizaciones deben cumplir con requerimientos de calidad, regulatorios y de seguridad, tanto para su información, como para sus activos. La administración debe obtener un balance adecuado en el empleo de los recursos informáticos que se muestran en la siguiente figura.

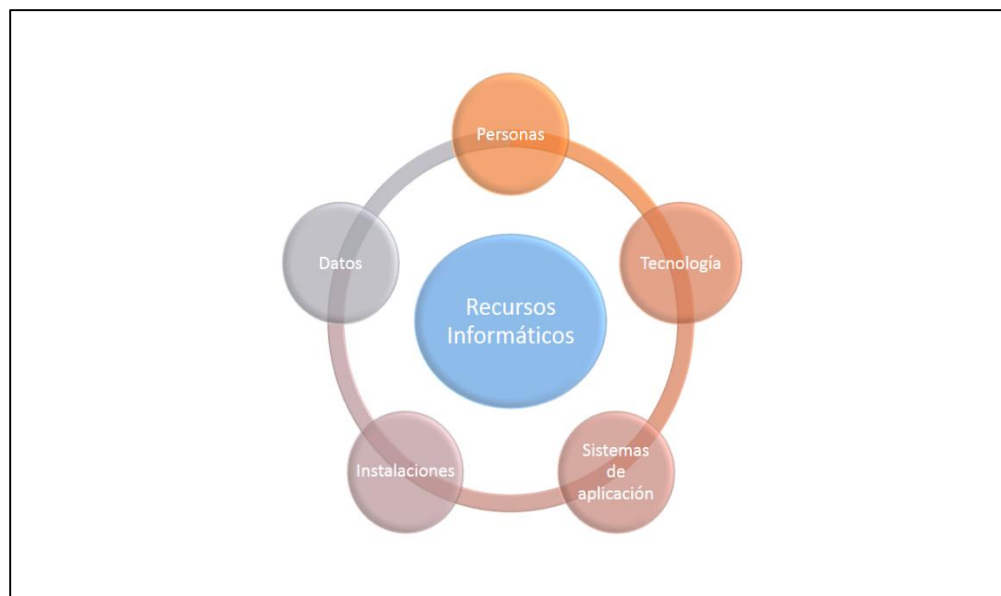


Figura 4 Recursos informáticos

Para cumplir con esa responsabilidad, así como para alcanzar sus expectativas, la administración debe establecer un sistema adecuado de control interno. Por lo tanto, ese sistema debe existir de modo que brinde soporte a los procesos de negocio y debe ser preciso en la forma en que cada actividad individual de control satisface los requerimientos de información y puede impactar en los recursos de tecnología de información. El impacto en los recursos de tecnología

de información se enfatiza en el Marco de Trabajo de COBIT, conjuntamente al logro de los siguientes requisitos indispensables para la información del negocio:

- Efectividad.
- Eficiencia.
- Confidencialidad.
- Integridad.
- Disponibilidad.
- Cumplimiento.
- Confiabilidad.

La Administración por medio del Gobierno Corporativo (Corporate Governance, en inglés), debe asegurar que la debida diligencia (due dilligence, en inglés) sea ejercitada por todos los individuos involucrados en la administración, utilización, diseño, desarrollo, mantenimiento u operación de los sistemas de información. (Dionicio Teo, 2011).

Un Objetivo de Control de Tecnología de Información es una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control específicos dentro de una actividad de tecnología de información.

La orientación a negocios es el tema principal de COBIT. Está diseñado no solo para ser utilizado por usuarios y auditores, sino también para ser utilizado como una lista de verificación (check list) detallada para los propietarios de los procesos del negocio. En forma creciente, las prácticas del negocio requieren de una mayor delegación y otorgamiento de autoridad de los dueños de procesos para que estos posean total responsabilidad de todos los aspectos relacionados con dichos procesos de negocio. En forma particular, esto incluye el proporcionar controles adecuados. El Marco de Trabajo de COBIT, proporciona herramientas al propietario del proceso para facilitarle el cumplimiento de esa responsabilidad. (Dionicio Teo, 2011).

La administración de una empresa requiere de prácticas generalmente aplicables y aceptadas de control y gobierno de tecnología de información para medir comparativamente, tanto su ambiente de tecnología de información existente, como su ambiente planeado. COBIT habilita el

desarrollo de una política clara y de mejores prácticas de control de tecnología de información a través de organizaciones a nivel mundial. El objetivo de COBIT es proporcionar estos objetivos de control, dentro de un marco de trabajo definido, y obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales del mundo.

Por lo tanto, COBIT está orientado a ser la herramienta de Gobierno de Tecnología de Información que ayude al entendimiento y la administración de riesgos asociados a la tecnología de información y tecnologías relacionadas. (Dionicio Teo, 2011).

El marco de trabajo COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos. Este principio, propio de COBIT 5, convalida su aplicabilidad a los sistemas de registros contables informáticos en correspondencia con las leyes vigentes. (Graciela Braga, 2015).

El gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas. (Graciela Braga, 2015).

1.10.4 Modelo de Madurez

Los modelos de madurez para el control de los procesos de TI consisten en desarrollar un método de puntaje de modo que una organización pueda calificarse a sí misma desde inexistente hasta optimizada (de 0 a 5).

COBIT 5 introduce una nueva forma de medir la madurez de los procesos a través del “Process Capability Model”, basado en el estándar internacionalmente reconocido “ISO/IEC 15504 Software Engineering – Process Assessment Standard”, diferente en su diseño y uso al modelo de madurez que incluía COBIT 4.1. ISACA. (2011).

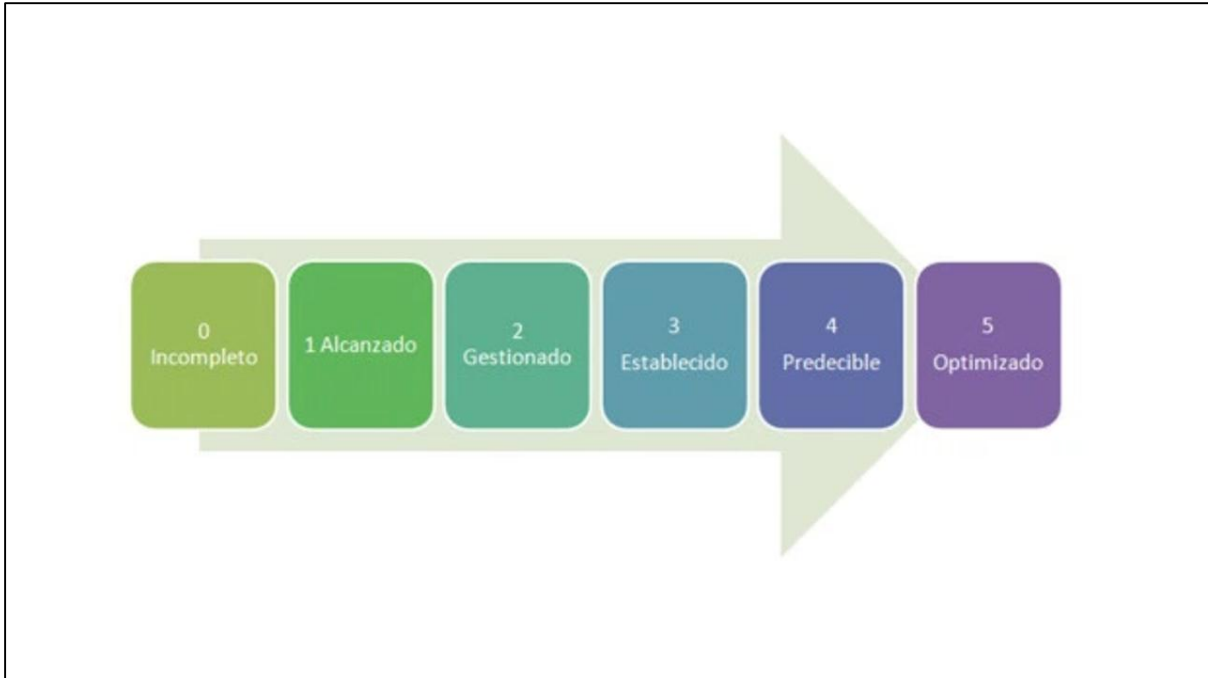


Figura 5 Modelo de Madurez "Process Capability Model" de COBIT 5. ISACA. (2011).

Incompleto: El proceso no está implementado o no alcanza su propósito. A este nivel hay muy poca o ninguna evidencia de algún logro sistemático del propósito del proceso.

Alcanzado: El proceso implementado alcanza su propósito.

Gestionado: El proceso ejecutado está implementado de forma gestionada y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.

Establecido: El proceso gestionado ahora está implementado usando un proceso definido que es capaz de alcanzar sus resultados de proceso.

Predecible: El proceso establecido ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso.

Optimizado: El proceso predecible es mejorado de forma continua para cumplir con los metas empresariales presentes y futuras.

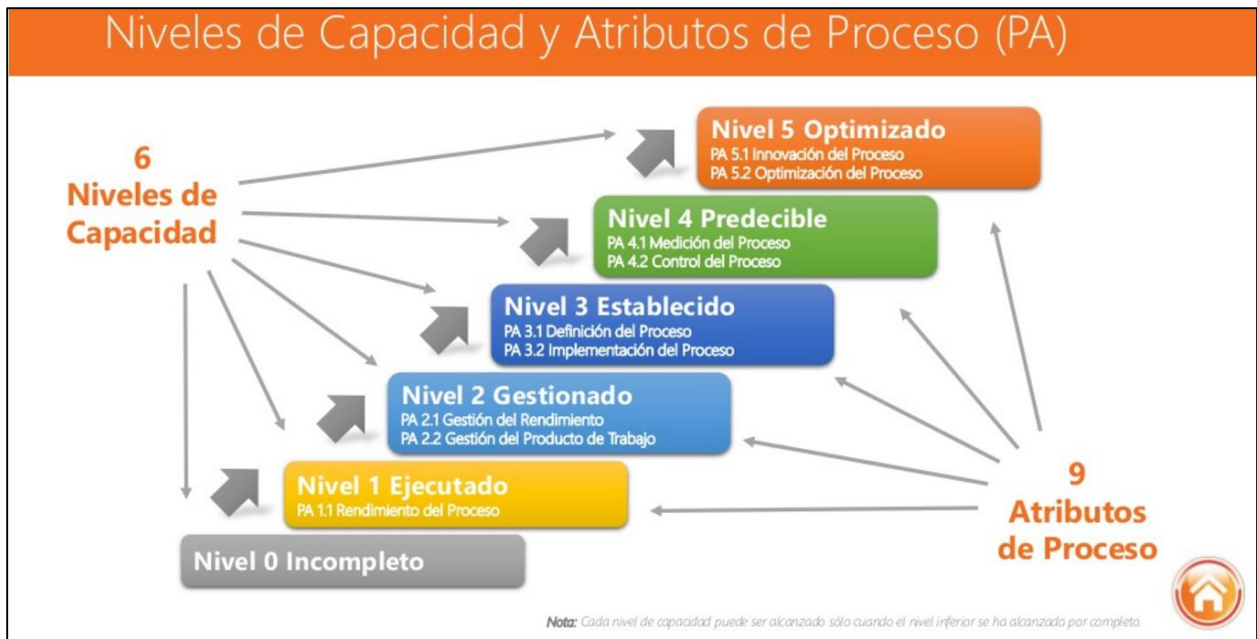


Figura 6 Niveles de capacidad y atributos de procesos. (Armenta Fonseca, 2014)

Las escalas del Modelo de Madurez ayudarán a la gerencia de usuarios a explicar a los administradores dónde existen deficiencias en la administración de TI y a fijarse objetivos para fortalecerlas de la mejor forma. El nivel correcto de madurez estará influenciado por los objetivos de negocio y el entorno operativo de la empresa. Específicamente, el nivel de madurez de control dependerá de la dependencia de TI que tenga la empresa, de la sofisticación de la tecnología y del valor de su información. (IT Governance).

Para concluir con el análisis de Madurez, es importante destacar que la decisión de una organización de invertir en la mejora de los procesos TIC debe estar basada en la comprensión de la importancia estratégica para cada uno de sus objetivos. El resultado de esta evaluación permitirá diseñar un plan de acción para la optimización de los procesos y recursos de la gestión TIC. (Orta Pedroza, 2014).

Para ello se debe desarrollar una lista de prioridades de los objetivos que requieren mayor atención, y a través de las buenas prácticas aplicables en el dominio de interés optimizar su gestión. Luego se puede alinear esta lista con la estrategia de la empresa, lo que permitirá comenzar a recorrer el camino a la mejora organizacional. (Orta Pedroza, 2014).

CAPÍTULO II ANÁLISIS SITUACIONAL DE LA COOPERATIVA DE AHORRO Y CRÉDITO NUEVA ESPERANZA

2.1 INTRODUCCIÓN

Durante el desarrollo de este capítulo se realizará el análisis situacional de la Cooperativa de Ahorro y Crédito Nueva Esperanza, esto es, su descripción, su infraestructura, cómo está organizada estructuralmente, cómo está conformada su área de sistemas, cómo está estructurada físicamente, qué sistema se utiliza y sobre qué base de datos trabaja, cuál es su plataforma de desarrollo, productos y servicios que ofrece, entre otros temas, que proporcionarán una idea general de la misma, tratándose de la empresa en la cual se desarrolla el presente trabajo de diploma.

Con estos conocimientos previos se define la problemática, se establece el plan de auditoría informática, el cual contempla el objetivo principal, el alcance de la auditoría, quién va realizar la auditoría y qué personas estarán involucradas.

Además se definen los principales procesos que se realizan en el departamento de Sistemas de la Cooperativa, posteriormente se realiza la elección de los procesos correspondientes a los dominios del marco referencial COBIT, estos han sido seleccionados en base al criterio del auditor para realizar la auditoría informática.

2.2 PROBLEMÁTICA

Uno de los problemas que se afrontan en la realización de auditorías informáticas a unidades financieras en el cantón Riobamba, es que no existe implementada una metodología que rija o norme los requisitos, pasos, esquemas y métodos para la aplicación de las tecnologías de la información con el fin de realizar las auditorías informáticas, según nos reportan autores como Naranjo y Freire en sus estudios realizados en los años 2010 y 2011. (Naranjo, 2010), (Freire, 2011).

Es por ello que la Cooperativa de Ahorro y Crédito Nueva Esperanza dentro del proceso de planificación y mejoramiento de la calidad de sus servicios ha tomado como un hito principal realizar un adecuado seguimiento y control de los procesos de negocio, principalmente en el departamento de Sistemas.

Para esto se ha establecido como proceso inicial la realización de una auditoría informática a dichos procesos, tomando como marco de trabajo a COBIT, para de esta forma verificar el cumplimiento de las normativas de la cooperativa dentro del departamento de Sistemas, y a partir de este estudio encontrar las diferentes falencias y proponer posibles mejoras que puedan adoptarse en la institución, y de la misma manera, asegurar que el sistema informático cumpla con los requerimientos de la entidad, permitiendo un adecuado manejo y control de los procesos de TI.

2.3 ANTECEDENTES

La Cooperativa de Ahorro y Crédito Nueva Esperanza, nace de la construcción y acción de sueños de varios chimboracenses que buscan el desarrollo sostenible y justo de su pueblo, durante estos 5 años de trabajo ha podido consolidar la generación de oportunidades a los sectores más desprotegidos y olvidados de la sociedad, como agricultores, artesanos, mujeres, niños, jóvenes, migrantes.

El sistema que utiliza la Cooperativa de Ahorro y Crédito Nueva Esperanza tiene por nombre “Sistema Financiero” el cual posee módulos operativos, módulos administrativos, módulos de control, módulos adicionales e interfaces externas. Este sistema es centralizado ya que se encuentra localizado en un servidor, y por ende todas las terminales acceden a éste para cualquier operación que se desee efectuar.

La cooperativa posee tres servidores, uno para la base de datos el cual trabaja con el sistema operativo LINUX REDHAT 6, otro servidor HP de Aplicaciones que tiene el Sistema Operativo WINDOWS SERVER 2012, donde está instalado el Sistema Financiero y el Reports Servers (para poder Imprimir y realizar Reportes). Y el tercero, un servidor de Internet que trabaja con el Sistema Operativo CentOS 6. Manual de Contingencias.

La página web de la Cooperativa de Ahorro y Crédito Nueva Esperanza contiene toda la información correspondiente a dicha cooperativa, en lo que respecta a su misión, visión, productos financieros, servicios, proyectos e información financiera.

La cooperativa cuenta con un departamento de auditoría interna, pero en él no existe una persona que se encargue específicamente de realizar una auditoría informática.

Las personas involucradas en el desarrollo de esta auditoría son:

- Gerente general: para apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.
- Jefe de sistemas y asistente técnico operativo: para identificar los controles que requieren en cada una de sus áreas.
- Los usuarios finales: quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.

Esta guía de auditoría informática servirá como una herramienta, tanto para el departamento de Sistemas, como para el departamento de auditoría interna de la Cooperativa de Ahorro y Crédito Nueva Esperanza, la cual permitirá efectuar evaluaciones periódicas no solo al área de Sistemas, sino a otras áreas que la requieran.

2.4 INFORMACIÓN DE LA INSTITUCIÓN

La Cooperativa de Ahorro y Crédito Nueva Esperanza es una institución de derecho privado, conformada por personas naturales sin propósito de lucro, que planifica y ejecuta actividades inherentes a sus principios, fines y objetivos. Uno de los objetivos es promover el espíritu cooperativista entre los ciudadanos de nuestra provincia y realizar actividades que busquen el mejoramiento económico social y profesional de sus socios.

La Institución inició sus labores un 7 de Abril del 2008, ofreciendo productos financieros y atendiendo a toda clase de clientes que han buscado un respaldo económico. Desde entonces vienen laborando, satisfaciendo las diversas necesidades de sus socios durante más de dos años de constitución.

La Cooperativa ha estado creciendo día a día gracias al apoyo, esfuerzo y empoderamiento que han tenido los empleados y socios dentro de la misma. Por otra parte la institución es sede de la presidencia de la Red de Finanzas Populares y Solidaria de Chimborazo lo cual hace que sea más reconocida y sólida a nivel Provincial.

La Cooperativa está dirigida a la prestación de servicios financieros y no financieros, a través de las actividades de captaciones, colocaciones y servicios complementarios que satisfagan las necesidades de socios y clientes en sus oficinas operativas.

Actualmente se encuentra trabajando bajo la los principios cooperativos como guía de trabajo, manteniendo así como lema “Cooperativismo a otro nivel” Manual de Perfiles (2012).

2.4.1 MISIÓN INSTITUCIONAL

Brindar servicios financieros y no financieros de alta calidad a los socios, enfocados a sectores populares y productivos de los chimboracenses que no han tenido acceso al sistema financiero tradicional, en cumplimiento a los principios cooperativos para fomentar el desarrollo económico social de la comunidad y promover la economía solidaria, con el trabajo comprometido y competitivo de su equipo humano y el apoyo de herramientas tecnológicas de vanguardia.

2.4.2 VISIÓN INSTITUCIONAL

Ser una cooperativa solvente con propias metodologías de trabajo, contando con personal y directivos comprometidos con un alto nivel de conocimiento y experticia identificada por todos los chimboracenses por su aporte a la consolidación de los procesos, encadenamientos productivos y articulación al proceso de desarrollo local sostenible basado en el ser humano y su desarrollo de capacidades con la formación de futuros líderes cooperativistas, posicionados en el mercado como un modelo cooperativo exitoso que se caracterice por el empoderamiento de sus socios y socias.

2.4.3 VALORES INSTITUCIONALES

- Honestidad
- Seguridad y compromiso

- Transparencia
- Agilidad y eficiencia
- Responsabilidad social
- Integridad
- Trabajo en equipo
- Flexibilidad operativa

2.4.4 OBJETIVOS INSTITUCIONALES

Objetivos generales

- Fortalecer el patrimonio institucional.
- Mejorar la atención al socio y cliente.
- Mantener autonomía e independencia.
- Integrar a los socios con la institución.
- Mejorar cooperación entre cooperativas.

Objetivos específicos

- Obtener un crecimiento sostenido y transparente de activos y pasivos.
- Realizar el manejo eficiente de la cartera de crédito y su morosidad.
- Mantener costos de operación mínimos.
- Adquirir la tecnología adecuada para servir mejor al socio, así como para contrarrestar el riesgo operativo.
- Ofrecer a nuestros socios y ciudadanía en general calidad en los productos y servicios con bajos costos para obtener ventaja competitiva.
- Crear productos innovadores acorde con los requerimientos de nuestros socios y ciudadanía en general.
- Mejorar el ambiente laboral, donde el personal desenvuelva sus capacidades de manera eficiente.
- Implementar un plan de capacitación continua al personal de la institución con el fin de alcanzar objetivos en común con la cooperativa.

- Establecer normas que permitan reducir gastos para tener mejores resultados al final de cada periodo.
- Elaborar un plan de publicidad dirigido a todos los socios para mantener al socio informado de los nuevos servicios y beneficios que ofrece la cooperativa.
- Realizar el presupuesto estructurado para la construcción del edificio casa matriz de la cooperativa, aprovechando que se cuenta con el terreno ubicado en el centro de la ciudad.
- Realizar el control periódico del desempeño de los concejos y comisiones de la cooperativa con el fin de que cumplan sus funciones de manera eficiente.
- Implementar una red de cajeros automáticos en las instalaciones de la cooperativa.
- Desarrollar el plan de contingencias para la recuperación de información en caso de desastres informáticos con el fin de eliminar el riesgo operativo.

2.4.5 PRODUCTOS Y SERVICIOS

- Ahorros
Son los depósitos a la vista que efectúan los socios a los cuales se les paga una tasa de interés acorde al mercado, sobre el saldo que mantenga en su libreta.
- Ahorro Futuro, Ahorro Mi Hogar, Ahorro Cesantía, Ahorro Minisosisio
Es un ahorro programado cooperativo al cual se le paga una de interés preferencial siempre que se encuentre dentro del mercado, los depósitos que realizan en éste producto son mensuales y se pueden disponer de ellos al año de aportaciones.
- Ahorro cooperativo
Son los depósitos a corto y mediano plazo, que realizan socios y clientes, a los cuales se les paga una tasa de interés acorde al mercado.
- Créditos
La cooperativa ofrece una variedad de créditos a sus socios, así como: créditos de consumo, comercio, microcrédito y vivienda, con garantías personales, garantía hipotecaria y garantía prendaria y garantía de aval.
- Garantías cooperativas
Es un aval que la cooperativa emite a favor de los profesionales de la construcción, para garantizar el trabajo que desarrollen con instituciones públicas o privadas.

- Pago de servicios básicos

La cooperativa ofrece a sus socios el pago de servicios a través de las libretas de ahorros, con los descuentos por el consumo que realizan tanto de luz, teléfono, agua potable.

2.4.6 INFRAESTRUCTURA

Actualmente la cooperativa tiene una oficina matriz ubicada en la ciudad de Riobamba, en Venezuela y Francia esquina 28-60 Francia.

2.4.7 ORGANIGRAMA ESTRUCTURAL

La Cooperativa de Ahorro y Crédito Nueva Esperanza se encuentra estructurada según lo muestra el organigrama de la Figura 7 donde se muestra que la organización se rige por jerarquías para definir sus niveles de dirección.

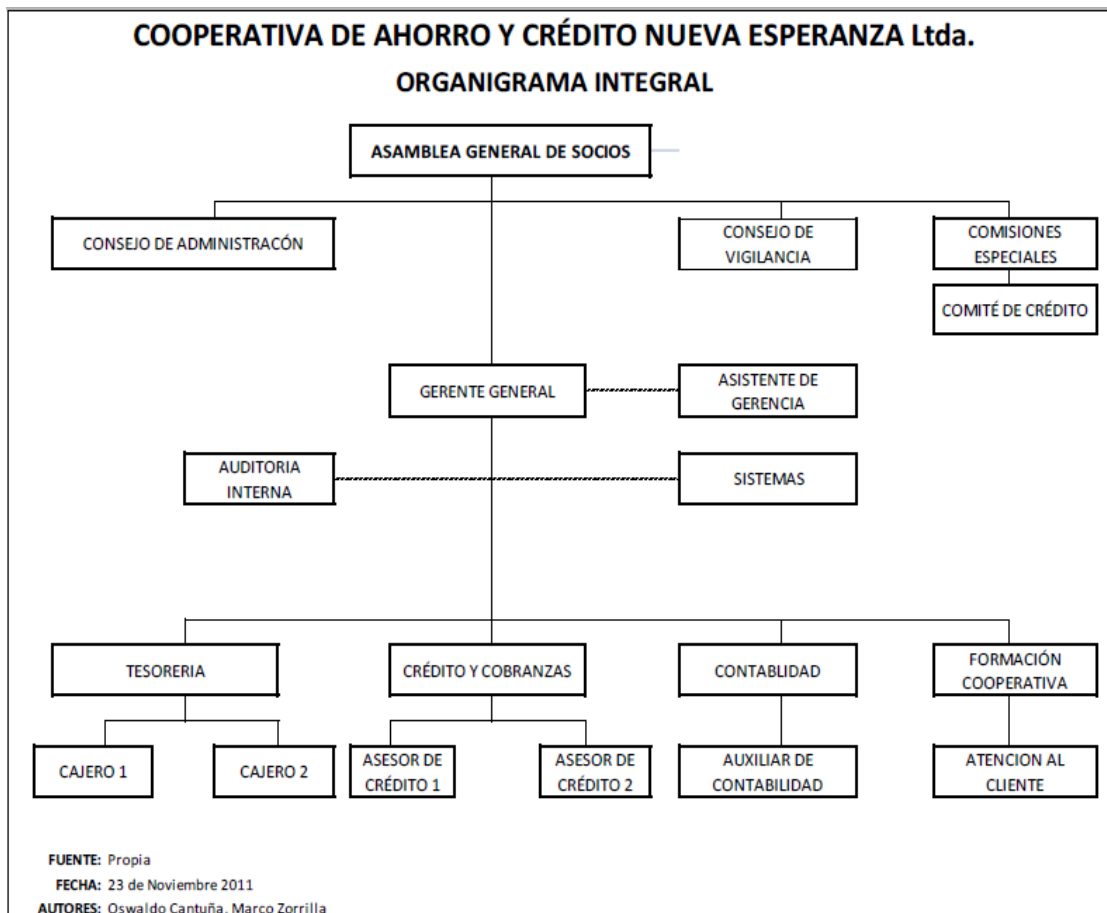


Figura 7 Organigrama General de la Cooperativa. Manual de Perfiles (2012).

2.4.8 DEPARTAMENTO DE SISTEMAS

El departamento de sistemas de la Cooperativa de Ahorro y Crédito Nueva Esperanza se encuentra conformado por el siguiente personal:

- Jefe de sistemas
- Operador de sistemas.

Estas personas son las encargadas de llevar a cabo las actividades relacionadas con la gestión informática de la Cooperativa.

El Departamento de Sistemas es el encargado del correcto funcionamiento de todos los recursos y servicios informáticos de la institución. Las principales funciones que desempeña dicho departamento son analizar, planificar, organizar, dirigir, controlar, implementar y evaluar el Sistema Financiero de la Cooperativa, permitiendo prestar los servicios financieros con la calidad requerida. Además tiene la responsabilidad de colaborar en la administración y desarrollo de los sistemas informáticos, dar soporte y mantenimiento a la infraestructura tecnológica y garantizar la seguridad de la información, así como atender los requerimientos de TI que presentan los clientes de la Cooperativa.

2.5 ESTRATEGIA

Con el objetivo de evaluar el control de los procesos fundamentales de la Cooperativa de Ahorro y Crédito Nueva Esperanza, ha surgido la necesidad de desarrollar e implementar una guía para la aplicación del modelo COBIT para las auditorías informáticas.

2.5.1 ALCANCE

El alcance de la presente evaluación está determinada por los procesos de los cuatro dominios como son:

Evaluar, dirigir y documentar, alinear, planear y organizar, construir, adquirir e implementar, entregar, servir y soportar del marco referencial COBIT en el ámbito de los procesos informáticos de La Cooperativa de Ahorro y Crédito Nueva Esperanza.

2.5.2 EQUIPO AUDITOR

Patricia Alexandra Badillo Pinto

2.5.3 INVOLUCRADOS

- Gerente General
Oswaldo D. Cantuña Adriano
- Jefe de sistemas
Lorena A. Moreno A
- Coordinador de Agencia
Luis Mosquera
- Contador General
Jaqueline Mera

2.6 SEGURIDAD INFORMÁTICA

2.6.1 FÍSICA

La Institución dispone de personal de seguridad en su entrada y en el área de Operaciones. Si es necesario el ingreso de personal externo al departamento de Sistemas, se lleva un registro que maneja el Jefe del departamento, en el que se refleja el nombre de la persona externa, fecha y hora de ingreso junto a su firma.

En el caso del área de servidores, el ingreso es restringido solo al personal que labora en el departamento de Sistemas. Cuenta con temperatura adecuada, no filtración de agua y detector de humo. Si es necesario el ingreso de personal ajeno, se registran los datos de la persona en una bitácora.

2.6.2 LÓGICA

Las estaciones de trabajo cuentan con contraseñas de acceso y los perfiles de usuarios se definen de acuerdo al rol que desempeña cada trabajador en la Cooperativa.

El uso de internet es restringido para uso personal. Cada usuario puede acceder a los sitios que se relacionen a las actividades que realiza en la Cooperativa.

No se permite el uso de puertos USB ni el almacenamiento de información ajena a la Cooperativa.

La única persona que tiene acceso a la configuración de los servidores es el Jefe de Sistemas, ya que es la persona que maneja las contraseñas.

2.6.3 DATOS

El proceso de respaldo de datos es responsabilidad del Departamento de Sistemas y se realiza mediante Scripts.

2.6.4 PERSONAL

En la Cooperativa rige el Reglamento Interno con el que tiene que cumplir el personal que labora en la misma. Donde se especifican las funciones de laborales y de disciplina con las que debe cumplir cada trabajador.

El departamento de Recursos Humanos es el encargado del proceso de contratación de personal nuevo, para esto está estipulado que debe existir un contrato donde se especifiquen los derechos y deberes del trabajador.

2.7 HIPÓTESIS

El uso de una guía de implementación de las tecnologías de la información, aplicando el modelo COBIT, para auditorías en entidades financieras permite la disminución de errores en su proceso de aplicación.

2.8 IDENTIFICACIÓN DE VARIABLES

2.8.1 VARIABLE INDEPENDIENTE

Guía para la implementación del modelo COBIT para auditoría en instituciones financieras.

2.8.2 VARIABLE DEPENDIENTE

Eficiencia en la gestión de las TIC en la aplicación de la auditoría informática usando una guía de implementación del modelo COBIT.

CAPÍTULO III GUÍA DE IMPLEMENTACIÓN APLICANDO COBIT

3.1 GUÍA DE IMPLEMENTACIÓN

Con el objetivo de proporcionar una guía que facilite la implementación del COBIT 5 en la Cooperativa de Ahorro y Crédito Nueva Esperanza, se definió una guía de implementación del modelo.

Finalmente, la base para la guía de implementación del modelo, se definieron las siguientes fases:

1. Definir tareas y responsables.
2. Identificar los procesos de la Cooperativa que se van a evaluar.
3. Definición de dominios y procesos de COBIT 5.
4. Selección de los procesos de COBIT asociados a los procesos de la Cooperativa.
5. Ejecución de la evaluación.

3.2 DEFINIR TAREAS Y RESPONSABLES.

Se presenta a la gerencia de la Cooperativa las tareas que se van a realizar, los responsables de la implementación de cada tarea y las actividades correspondientes a cada uno.

Para lograr este objetivo es necesario presentar el modelo a la gerencia, explicar el alcance del proyecto, definir los roles y responsables de cada actividad, así como el cronograma de implementación del proyecto e informar a las partes interesadas. (Anexo 1).

3.2.1 GRUPO EVALUADOR

Para la ejecución de la auditoría es necesario definir un grupo de trabajo que conozca detalladamente su área y su relación con el Departamento de Sistemas de la Cooperativa. En nuestro caso hemos seleccionado a los jefes de los departamentos que son considerados más críticos para el cumplimiento de los objetivos trazados.

En la Tabla 1 se muestra el grupo evaluador seleccionado para llevar a cabo este trabajo dada su experiencia y conocimiento.

Grupo evaluador	
Cargo	Nombre
Gerente General	Oswaldo D. Cantuña Adriano
Jefe de sistemas	Lorena A. Moreno A
Coordinador de Agencia	Luis Mosquera
Contador General	Jaqueline Mera
Evaluadora	Patricia Alexandra Badillo Pinto

Tabla 1 Grupo evaluador.

A continuación se describen brevemente las funciones de cada integrante del grupo evaluador:

Gerente general

La principal responsabilidad que ejerce es la de ser el máximo representante de la Cooperativa. Es quien propone al Consejo de Administración las políticas, reglamentos y procedimientos para el buen funcionamiento de la Cooperativa, además de las propuestas de plan estratégico y operativo junto con su proforma presupuestaria. Define y mantiene el control interno para la eficiente gestión económica de la Cooperativa. Manual de Perfiles.

Jefe de sistemas

Sus principales funciones son analizar, planificar, organizar, dirigir, controlar, implementar y evaluar el sistema financiero de la Cooperativa, permitiendo la prestación oportuna de los

servicios que brinda la Cooperativa a sus clientes. Además se encarga del mantenimiento de la infraestructura y recursos de TI necesarios para el correcto funcionamiento de la Cooperativa.

Coordinador de Agencia

Responsabilizar la dirección y funcionamiento de las agencias como de su posicionamiento en cada una de las sucursales manejando una atención de calidad y fidelidad de los socios. Desarrolla estrategias generales para el incremento de clientes en la Organización, Realiza atención al cliente, inspecciona y revisa los créditos, etc. Manual de Perfiles.

Contador General

Entre las responsabilidades que tiene el Jefe de Contabilidad se destacan la ejecución del control previo de las transacciones financieras de la Cooperativa, supervisión del manejo adecuado de la información contable de la matriz y sucursales de la cooperativa. Debe llevar el control del manejo de la tesorería con el fin de que los fondos sean dirigidos y administrados con seguridad, así como la verificación diaria de los cajeros automáticos. Manual de Perfiles.

3.3 IDENTIFICAR LOS PROCESOS DE LA COOPERATIVA QUE SE VAN A EVALUAR.

Para realizar una evaluación de la Cooperativa de Ahorro y Crédito Nueva Esperanza aplicando el modelo COBIT, se decidió evaluar los siguientes procesos.

- Gestión de recursos físicos
- Gestión de talento humano
- Gestión de operaciones
- Gestión de contabilidad
- Gestión de planificación estratégica
- Gestión de tecnología y recursos de TI
- Gestión de control interno y regulaciones externas
- Gestión de marketing
- Gestión de información

3.4 DEFINICIÓN DE DOMINIOS Y PROCESOS DE COBIT 5.

COBIT 5 define la manera de implementar las buenas prácticas de Gobierno y Gestión de TI en las instituciones proponiendo un modelo de referencia que consta de 37 procesos, los cuales deberán ser analizados y evaluados para definir cuáles de estos son necesarios para aumentar su competitividad y lograr eficiencia operativa, como se muestra en la Figura 8.

La confección de esta metodología posibilitaría un mejor control de la información que disponen las unidades bancarias y a la vez implicarían una considerable disminución de riesgos en cuanto a fuga de información se refiere.

La presente guía de implementación del modelo COBIT brinda unificación en el proceso de su aplicación y reducirá los niveles de errores en su aplicación y resultados, lo que se traduciría en mayor seguridad de la información contable y con esto menor daño para clientes internos y externos.

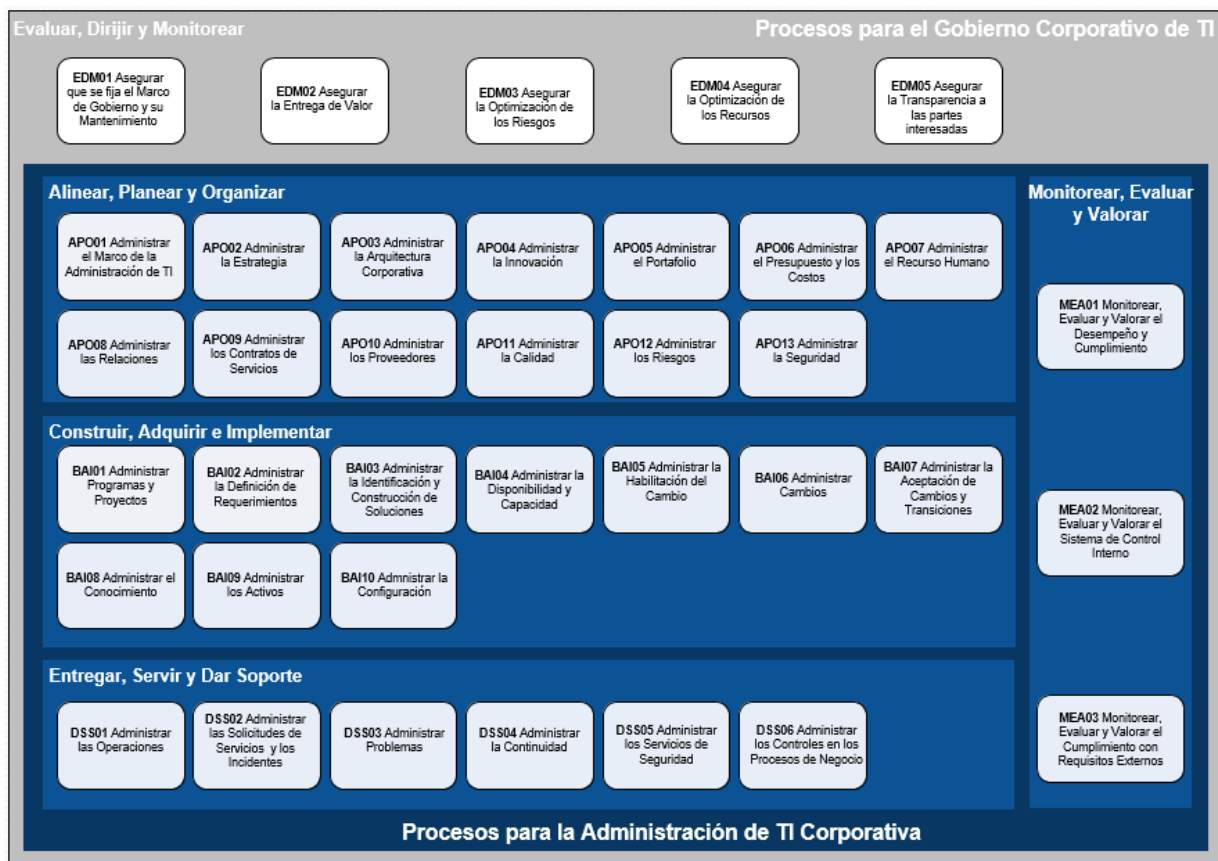


Figura 8 Procesos de COBIT 5. (COBIT 5 (2012)).

3.5 DEFINICIÓN DE DOMINIOS COBIT.

Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados. Habitualmente se ordenan dentro de dominios de responsabilidad de planificar, construir, ejecutar y monitorear que proponen a la Cooperativa de ahorro y Crédito Nueva Esperanza un modelo mejorado de procesos de TI alineado a las metas del negocio.

1. Evaluar, Orientar y Supervisar. (EDM)
2. Alinear, Planificar y Organizar. (APO)
3. Construir, Adquirir e Implementar. (BAI)
4. Entregar, Dar servicio y Soporte. (DSS)
5. Supervisar, Evaluar y Valorar. (MEA)

3.6 SELECCIÓN DE LOS PROCESOS DE COBIT ASOCIADOS A LOS PROCESOS DE LA COOPERATIVA.

Para la realización de esta guía es fundamental definir y seleccionar los dominios y procesos en los que se va a apoyar la evaluación, teniendo en cuenta las características, objetivos y metas del Departamento de Sistemas de la Cooperativa de Ahorro y Crédito Nueva Esperanza.

Es importante señalar que la Cooperativa no dispone de un levantamiento de procesos ni documentación que los respalde, por lo que los procesos definidos se basan en las funciones que desempeña cada departamento dentro de la Institución.

Teniendo en cuenta los criterios de información de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento de regulaciones, y confiabilidad, que propone COBIT 5, se determinaron los procesos críticos de TI y se establecieron las relaciones con los procesos propios del marco COBIT 5.

A continuación se presenta la guía del modelo de mejoramiento de procesos de TI que se recomienda implementar en la Cooperativa de Ahorro y Crédito Nueva Esperanza.

Los procesos de Gobierno que se propone aplicar son los siguientes: EDM01, EDM02, EDM03 y EDM04.

Gestión de ti

A pesar que los procesos de la Cooperativa están desarrollados de manera empírica y con una débil definición, se adaptan a los procesos que recomienda COBIT 5.

Los procesos de Gestión de TI, que se obtienen a partir del análisis del marco de COBIT 5, que se recomiendan fortalecer en la Cooperativa de Ahorro y Crédito Nueva Esperanza son: APO01, APO02, APO03, APO04, APO07, APO11, APO12, BAI02, BAI03, BAI05, DSS04, DSS05, MEA01, MEA02 y MEA03.

En la tabla 1 se muestran los procesos más relevantes de la Cooperativa de Ahorro y Crédito Nueva Esperanza relacionados con los procesos que COBIT 5 propone.

MAPEO DE LOS PROCESOS DE LA COOPERATIVA CON LOS PROCESOS DE COBIT 5		
MACRO-PROCESOS	PROCESOS	PROCESOS ASOCIADOS A COBIT 5
1. Gestión de Recursos físicos.	<ul style="list-style-type: none"> • Identificar y adquirir Recursos físicos. • Gestionar condiciones de adquisición de recursos físicos. • Dar soporte a recursos físicos. • Inventariar recursos físicos. 	<ul style="list-style-type: none"> • APO12 Administrar los riesgos • APO01 Administrar el marco de la administración de TI • BAI02 Administrar la definición de requerimientos • BAI03 Administrar la definición y construcción de soluciones • DSS04 Administrar la continuidad

		<ul style="list-style-type: none"> • DSS05 Gestionar los servicios de seguridad
2. Gestión de créditos.	<ul style="list-style-type: none"> • Asignar créditos. • Autorizar créditos. • Cancelar créditos. 	<ul style="list-style-type: none"> • DSS05 Gestionar los servicios de seguridad
3. Gestión de talento humano.	<ul style="list-style-type: none"> • Seleccionar y contratar personal. • Planificar capacitaciones al personal según el cargo. • Elaborar la organización funcional de departamentos. • Elaborar Manual de Perfiles de la Cooperativa. • Evaluar y monitorear periódicamente el desempeño del personal. 	<ul style="list-style-type: none"> • APO01 Administrar el marco de la administración de TI • APO11 Administrar la calidad
4. Gestión de operaciones.	<ul style="list-style-type: none"> • Receptar depósitos. • Efectuar retiros. • Cobrar servicios básicos. • Administrar caja general. • Realizar cuadros de operaciones. • Realizar transacciones financieras. 	<ul style="list-style-type: none"> • DSS05 Gestionar los servicios de seguridad
5. Gestión de contabilidad.	<ul style="list-style-type: none"> • Realizar cuadros diarios de caja general. • Manejar caja chica. 	<ul style="list-style-type: none"> • DSS05 Gestionar los servicios de seguridad

	<ul style="list-style-type: none"> • Controlar transacciones financieras. • Consolidar balances contables de la cooperativa. 	
6. Gestión de planificación estratégica.	<ul style="list-style-type: none"> • Desarrollar el plan estratégico. • Monitorear y actualizar el plan estratégico. • Definir iniciativas estratégicas para mejorar la atención al cliente y para impulsar la gestión de negocios de la cooperativa. • Identificar riesgos financieros. • Emitir informes de las actas a toda la organización. • Desarrollar planes de auditoría y control de gestión. • Realizar análisis de riesgos del negocio. • Comunicar el plan estratégico y operativo a todos los departamentos. 	<ul style="list-style-type: none"> • APO02 Administrar la estrategia • APO04 Administrar la innovación • APO03 Administrar la Arquitectura Corporativa • APO01 Administrar el marco de la administración de TI • APO11 Administrar la calidad • APO12 Administrar los riesgos • DSS04 Administrar la continuidad • MEA02 Monitorear, evaluar y valorar el sistema de control interno
7. Gestión de tecnología y recursos de TI.	<ul style="list-style-type: none"> • Dar soporte y mantenimiento a recursos de TI. 	<ul style="list-style-type: none"> • APO02 Administrar la estrategia • APO03 Administrar la arquitectura corporativa

<ul style="list-style-type: none"> • Mantener el sistema de información. • Atender requerimientos tecnológicos de los usuarios. • Administrar servicios de TI con terceros. • Realizar informes periódicos sobre recursos de TI para la toma de decisiones. • Monitorear el desempeño de los recursos de TI. • Coordinar actividades de las áreas del Departamento de Sistemas. • Capacitar a los usuarios acerca del uso de recursos de TI para el cumplimiento de sus funciones. • Comunicar sobre fallas de servicios a proveedores externos para su mantenimiento. • Monitorear red de comunicación entre todas las oficinas. • Implementar medidas de seguridad en los sistemas informáticos. • Analizar y reportar problemas de seguridad 	<ul style="list-style-type: none"> • APO01 Administrar el marco de la administración de TI • APO04 Administrar la innovación • APO11 Administrar la calidad • APO12 Administrar los riesgos • BAI02 Administrar la definición de requerimientos • BAI03 Administrar la definición y construcción de soluciones • BAI05 Administrar la habilitación del cambio • DSS04 Administrar la continuidad • DSS05 Gestionar los servicios de seguridad • MEA01 Monitorear, evaluar y valorar el desempeño y cumplimiento
--	---

	<p>detectados en el sistema financiero.</p> <ul style="list-style-type: none"> • Realizar respaldos de la base de datos antes y después del cierre del sistema financiero. • Realizar el cierre del sistema financiero. • Realizar y actualizar inventarios de equipos del Departamento de Sistemas. 	
<p>8. Gestión de control interno y regulaciones externas.</p>	<ul style="list-style-type: none"> • Identificar las leyes, regulaciones o disposiciones de los organismos de control que afectan a la organización. • Coordinar y aprobar las medidas para garantizar el cumplimiento de leyes, regulaciones o disposiciones identificadas. • Comunicar las medidas aprobadas a todos los involucrados. • Monitorear el cumplimiento de las medidas aprobadas. • Cumplir con las disposiciones de los Organismos de Control. 	<ul style="list-style-type: none"> • MEA02 Monitorear, evaluar y valorar el sistema de control interno • MEA03 Monitorear, evaluar y valorar el cumplimiento con requisitos internos

<p>9. Gestión de marketing.</p>	<ul style="list-style-type: none"> • Realizar la publicidad de la cooperativa para la capacitación de socios. • Desarrollar análisis de mercado. 	<ul style="list-style-type: none"> • BAI03 Administrar la definición y construcción de soluciones
<p>10. Gestión de información.</p>	<ul style="list-style-type: none"> • Capacitación sobre custodia y manejo de la información institucional. • Establecer medidas para garantizar la seguridad de la información institucional. • Elaboración de actas, disposiciones, aspiraciones o políticas emitidas por la Gerencia General. 	<ul style="list-style-type: none"> • APO03 Administrar la arquitectura corporativa • APO01 Administrar el marco de la administración de TI • DSS04 Administrar la continuidad • DSS05 Gestionar los servicios de seguridad • MEA03 Monitorear, evaluar y valorar el cumplimiento con requisitos internos

Tabla 2 Procesos de la Cooperativa de Ahorro y Crédito Nueva Esperanza asociados al marco de COBIT 5.

3.7 METODOLOGÍA

En esta fase se define los métodos, mecanismos, estrategias o procedimientos a seguirse en la investigación. A continuación se especifica sus componentes:

3.7.1 ESTUDIO DESCRIPTIVO

El método descriptivo es aquel, que como su nombre lo indica, describe una serie de actividades o sucesión de hechos necesarios para lograr el objetivo. En este caso particular estará plasmado en una guía para lograr la implementación del modelo COBIT para auditoria en instituciones financieras.

Se utilizará el método inductivo, al partir de una problemática como es la no existencia de una guía de implementación de las tecnologías de la información, específicamente del modelo COBIT, para la realización de auditorías en entidades financieras, para llegar a un resultado final que será la guía de implementación y una conclusión general, que es necesario implementar, para

administrar los recursos de tecnologías de la información, el modelo COBIT, para cualquier organización e institución financiera.

En este proyecto se utilizarán técnicas de recolección de la información primaria al utilizar los conocimientos adquiridos sobre auditoría de sistemas y también se utilizará la observación de datos estadísticos de la Cooperativa de Ahorro y Crédito Nueva Esperanza de la provincia de Chimborazo. La recolección de la información secundaria será a través de la utilización del modelo COBIT para la realización de auditorías a tecnologías de la información de las entidades financieras, además de utilizar artículos, libros y otros trabajos relacionados con el tema.

3.7.2 POBLACIÓN Y MUESTRA

Población

La población en este estudio estará compuesta por las instituciones financieras de la provincia de Chimborazo, especialmente por las 17 Cooperativas de Ahorro y Crédito existentes.

Muestra

La Cooperativa de Ahorro y Crédito Nueva Esperanza de la provincia de Chimborazo.

3.7.3 OPERACIONALIZACIÓN DE VARIABLES

En la tabla 3 se presenta la operacionalización conceptual y metodológica de las variables que se han identificado de acuerdo a la hipótesis.

VARIABLE	Tipo	DIMENSIÓN	INDICADORES
VI. Guía para la implementación del modelo COBIT para auditorías a instituciones financieras.	Independiente	Confeccionar una guía de implementación del modelo COBIT para la realización de auditorías en instituciones financieras.	<ul style="list-style-type: none"> • Confeccionada • No confeccionada

VD. Eficiencia en la gestión de las TIC en la aplicación de la auditoría informática usando una guía de implementación del modelo COBIT.	Dependiente	<ul style="list-style-type: none"> • Establecer un marco de trabajo de gobierno para TI. • Entrega de valor. • Administración de riesgos. • Medición del desempeño Aseguramiento independiente. 	<ul style="list-style-type: none"> • Seguridad de la información. • Disponibilidad de la información. • Actividades para la gestión interna de las TICs. • Actividades de Aseguramiento.
---	-------------	---	--

Tabla 3 Operacionalización de variables

Nota: se tomara como referencia el número de errores procedimentales encontrados en auditorías realizadas con anterioridad en las cuales no se aplicó el modelo COBIT.

3.7.4 PROCEDIMIENTOS

En el la siguiente Tabla identificamos los procesos que serán aplicados:

1. Estudio introductorio y análisis del modelo COBIT	Estudio teórico	Libros, Manuales, Guías	Material bibliográfico que sirva de referencia para conocer y entender el modelo COBIT de auditoria de tecnologías de la información.
2. Análisis de esquemas, métodos o guías a integrar	Estudio teórico práctico	Libros, Manuales, Guías	Material bibliográfico de esquemas, métodos de implementación o guías utilizadas para las auditorias de la tecnología de la información.
3. Determinación de esquemas, métodos o guías a incorporar en el proyecto	Estudio teórico práctico	Libros, Manuales, Guías	Análisis de esquemas, métodos o guías a incorporar de las varias recopiladas anteriormente

4. Identificación de los principales procesos a analizar por la guía de implementación	Estudio experimental, práctico	Recursos Metodológico	Análisis de los procesos a cubrir en la guía de implementación
5. Diseño de la estructura de la guía de implementación	Estudio experimental, práctico	Recursos Metodológico	Diseño y elaboración de la estructura de la guía de implementación.
6. Desarrollo del proyecto	Estudio experimental, práctico	Recursos Metodológico	Realizar auditoría aplicando la guía de implementación del modelo COBIT.
7. Identificación y corrección de errores	Estudio experimental, práctico	Recursos Metodológico	Identificación y análisis de errores encontrados en aplicación de la guía.

Tabla 4 Tabla de procedimientos

CAPÍTULO IV EJECUCIÓN DE LA EVALUACIÓN Y ANÁLISIS DE RESULTADOS

4.1 PLANIFICACIÓN DE LA EVALUACIÓN

Para llevar a cabo la evaluación de los procesos seleccionados en el capítulo anterior se utilizan directrices de auditoría de COBIT que permitirán realizar una síntesis de la situación actual con respecto a la Gestión de las TICs en la Cooperativa de Ahorro y Crédito Nueva Esperanza.

También se realizó un análisis del nivel de madurez de cada uno de los procesos que serán referenciados.

4.2 DIRECTRICES DE LA AUDITORÍA

Las directrices de auditoría planteadas para la realización de la presente auditoría permiten evaluar los controles, procesos, actividades y procedimientos que son realizados actualmente por el Departamento de Sistemas para dar cumplimiento a los objetivos de la Institución.

Proporcionan una guía que permite a los evaluadores definir el proceso de planificación y ejecución de la evaluación, teniendo en cuenta aspectos necesarios como el alcance, recolección de la información concerniente a los procesos involucrados, documentación necesaria para la evaluación, etc.

Como parte de las directrices COBIT propone un modelo de madurez genérico que permite determinar el nivel actual en el que se encuentra cada uno de los procesos a evaluar y puede ser de ayuda como guía para definir el nivel futuro en el que deberían dichos procesos.

Las escalas utilizadas se tomaron del marco de COBIT 5 y son las siguientes:

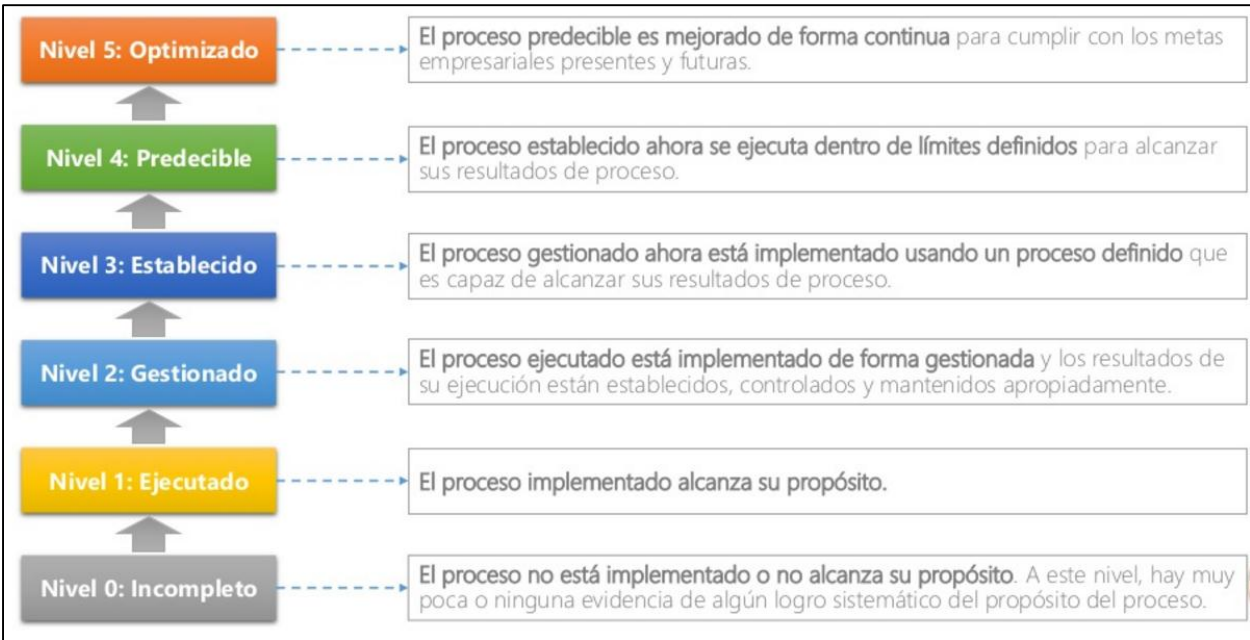


Figura 9 Niveles de Capacidad. (Orta Pedroza, 2014).

4.3 MEDICIÓN DEL NIVEL DE MADUREZ DE LOS PROCESOS

Para obtener la información necesaria para determinar el nivel de madurez de los procesos seleccionados se utilizan directrices de auditoría de COBIT.

Para realizar el análisis de los procesos se tuvo en cuenta la siguiente estructura para cada nivel de madurez en una escala de 0 a 5: No existe (0), Inicial (1), Repetible pero intuitivo (2), Definido (3), Administrado (4) y Optimizado (5).

Es necesario que el usuario atribuya un factor de peso (1 a 10) para indicar la importancia de cada una de las sentencias dentro de la organización y su ambiente interno y externo.

El usuario debe indicar a qué nivel se cumple con cada sentencia, usando las siguientes escalas:

- No se cumple en absoluto (Nada).
- Se cumple a un nivel limitado (Un poco).
- Se cumple a un nivel significativo (Algo).
- Se cumple completamente (Completamente).

Para calcular la importancia relativa de cada una de estas sentencias se debe multiplicar el peso por el nivel de cumplimiento de cada una.

En la Figura 9 se puede apreciar la estructura para el proceso APO02 Administrar la estrategia.

Los cálculos se realizaron de la siguiente forma:

Para calcular la importancia relativa se tiene en cuenta el peso que se asigna a cada sentencia en cada nivel de madurez por el valor que se le asigna a la sección “Está de acuerdo” (cumplimiento). Cada uno de los grados de esta sección tiene un valor entre 0 y 1 distribuidos de la siguiente forma:

- Nada tiene valor 0.
- Poco tiene valor 0,33.
- Algo tiene valor 0,66.
- Completamente tiene valor 1.

En la tabla que muestra el resultado final del cálculo global de nivel de madurez del proceso en cuestión, se toma en cuenta la importancia relativa para hallar el valor de aportación. Para el cálculo de la aportación se realiza un promedio de la importancia relativa de las sentencias por cada nivel de madurez dividido por el peso total de cada nivel de madurez. Este valor se multiplica por el valor asignado en la columna de cumplimiento.

Finalmente el nivel de madurez global se obtiene como resultado de la sumatoria de los valores obtenidos en cada nivel de madurez analizado.

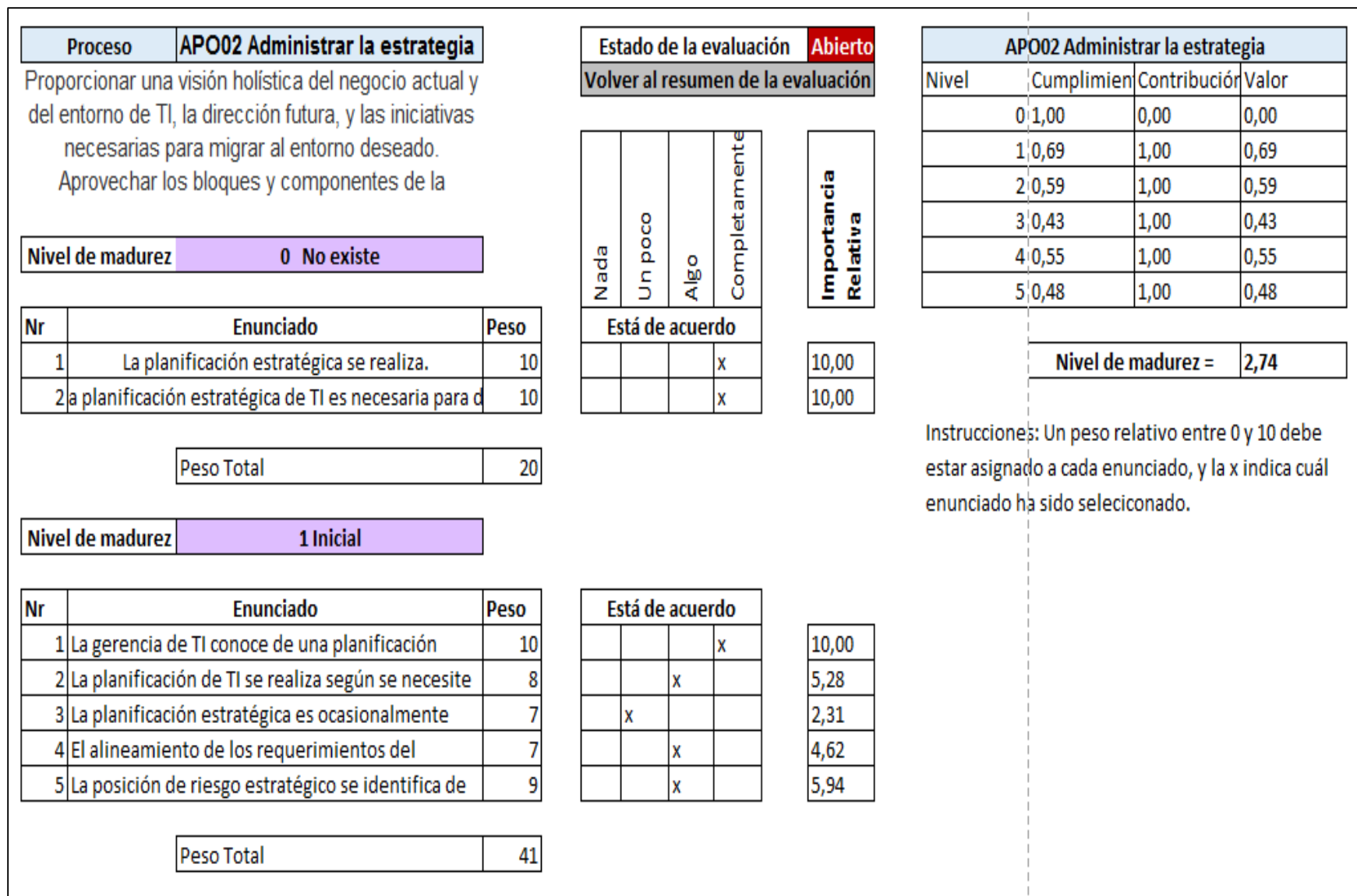


Figura 10 Ejemplo del cálculo del proceso APO02.

4.4 EJECUCIÓN DE LA EVALUACIÓN

4.4.1 ALINEAR, PLANIFICAR Y ORGANIZAR (APO)

4.4.2.2 APO01 GESTIONAR EL MARCO DE GESTIÓN DE TI.

Entradas	Si	Parcialmente	No	Observaciones
<p>Políticas y Procedimientos inherentes al proceso de planificación.</p> <ul style="list-style-type: none"> • Misión • Visión • Mapa estratégico • Estrategias tecnológicas 	X			
<p>Roles y Responsables del equipo de dirección</p> <ul style="list-style-type: none"> • Los propietarios de procesos y la Gerencia llevan a cabo revisiones y aprobaciones formales de los planes de TI. 		X		<ul style="list-style-type: none"> • Los roles y responsabilidades se encuentran definidos en el Manual de Perfiles de la Cooperativa. • No se tienen definidos procesos documentados, las actividades de cada departamento solo se basan en el reglamento general donde están definidas las políticas de la Cooperativa.
<p>Reportes y minutas de seguimiento de las reuniones de comité de Planificación y Dirección.</p>	X			<ul style="list-style-type: none"> • Se tienen actas y libros correspondientes de cada sesión realizada para la toma de decisiones de la organización.

Tabla 5 Directrices de auditoría de APO01.

4.4.2.3 APO02 ADMINISTRAR LA ESTRATEGIA

Entradas	Si	Parcialmente	No	Observaciones
<p>Objetivos y dirección de la Cooperativa.</p> <ul style="list-style-type: none"> • Los planes a corto y largo plazo de tecnología de información son consistentes con los planes a corto y largo plazo de la organización, así como con los requerimientos de ésta. 	X			<ul style="list-style-type: none"> • Para su cumplimiento se basa en los reglamentos internos de cada departamento además del crecimiento de la Cooperativa, satisfacción de los clientes, tendencias tecnológicas.
<p>Objetivos de Ti a largo y corto plazo</p> <ul style="list-style-type: none"> • Iniciativas de tecnología de información para soportar la misión y las metas de la organización. • Estudios de factibilidad de las iniciativas de tecnología de información. • Evaluación de los riesgos de las iniciativas de tecnología de información. • Inversiones óptimas en tecnologías de información actuales y futuras. • Los proyectos de TI están soportados por la documentación apropiada según lo 		X		<ul style="list-style-type: none"> • Las iniciativas de tecnología de información se transmiten a la Gerencia para ser aprobadas por el Comité Ejecutivo y luego el Consejo de Administración. Las iniciativas son generadas por experiencia del Jefe del Departamento de Sistemas y por necesidades del negocio. • Se realizan estudios internos de factibilidad basados en la satisfacción de requerimientos del Departamento de Sistemas, pero estos no cuentan con una documentación que los respalde, ni son formalmente aceptados. • Para la inversión en tecnología se tiene en cuenta el análisis costo-beneficios que realiza el departamento

definido en la metodología de planificación de tecnología de información.				<p>de Sistemas y de acuerdo a las necesidades de la Institución.</p> <ul style="list-style-type: none"> • No se tiene una metodología definida. Solamente se reportan documentos con los resultados del análisis costo-beneficios a la Gerencia y las razones por las que se solicita un determinado recurso. • Para conseguir las aprobaciones de los proyectos que se llevan a cabo, se realizan reuniones informales.
---	--	--	--	--

Tabla 6 Directrices de auditoría de APO02.

4.4.2.4 APO03. GESTIONAR LA ARQUITECTURA EMPRESARIAL.

Entradas	Si	Parcialmente	No	Observaciones
<p>Políticas y procedimientos sobre la arquitectura de información.</p> <ul style="list-style-type: none"> • Estándares internacionales. 		X		<ul style="list-style-type: none"> • No se tienen políticas o procedimientos definidos, se basan en estándares de la Institución, solo se rigen por el reglamento general y las políticas establecidas en la Cooperativa.
<p>Modelo de la arquitectura de información.</p> <ul style="list-style-type: none"> • El proceso utilizado para actualizar el modelo de la arquitectura de la información toma como base los planes a corto y largo plazo, considera los costos y riesgos asociados y asegura que las aprobaciones 		X		<ul style="list-style-type: none"> • Solo el Jefe del Departamento de Sistemas está autorizado para realizar modificaciones en la base de datos. Para una modificación en la arquitectura de la información se consulta con la Gerencia General.

formales de la Gerencia sean obtenidas antes de hacer modificaciones al modelo.				
<ul style="list-style-type: none"> • Documentos que soporten el modelo de la arquitectura de información, incluyendo el modelo de datos corporativo. 		X		<ul style="list-style-type: none"> • No existen documentos sobre la arquitectura de la información como el modelo de base de datos, sin embargo para realizar modificaciones en la base de datos se realizan registros en el documento de Pase a producción.
<p>Diccionario de datos corporativo.</p> <ul style="list-style-type: none"> • Reglas de sintaxis de datos. • Utiliza algún proceso para mantenerlo actualizado. 			X	<ul style="list-style-type: none"> • No existe a definición de un diccionario de datos corporativo.
<p>Política de propiedad de datos.</p> <ul style="list-style-type: none"> • Clasificación de los datos. • Categorías de seguridad. • Reglas de acceso. • La existencia de un proceso de autorización que requiera que el propietario de los datos autorice todos los accesos a los mismos. 		X		<ul style="list-style-type: none"> • Se aplica la seguridad a los datos mediante la implementación de perfiles de usuarios en el Sistema Financiero. • Dentro del módulo de Administración de usuarios del Sistema Financiero se implementan las reglas de acceso. • No cuentan con un proceso documentado de autorización que permita que el propietario de los datos deba autorizar todos los accesos a determinados datos.

Tabla 7 Directrices de auditoría de APO03.

4.4.2.5 APO04. GESTIONAR LA INNOVACIÓN.

Entradas	Si	Parcialmente	No	Observaciones
<p>Políticas y procedimientos relacionados con la planificación y el monitoreo de la infraestructura tecnológica.</p> <ul style="list-style-type: none"> • Existe un proceso para la creación y la actualización regular del plan de infraestructura tecnológica para confirmar que los cambios propuestos sean analizados antes de evaluar los costos y riesgos. 			X	<ul style="list-style-type: none"> • No se cuenta con un plan de infraestructura tecnológica independiente, sino que la planificación de la infraestructura se encuentra dentro del plan operativo anual. La evaluación de costos y riesgos se realiza internamente en el Departamento de Sistemas y sus resultados son presentados a la Gerencia General para su aprobación y toma de decisiones.
<p>Roles y responsabilidades de la Gerencia.</p> <ul style="list-style-type: none"> • La Gerencia aprueba el plan antes de realizar algún cambio. 	X			
<p>Objetivos y planes de la organización a largo y corto plazo.</p> <ul style="list-style-type: none"> • Identificar los costos y riesgos asociados, y que dichos cambios reflejen las modificaciones a los planes a largo y corto plazo de tecnología de información. 		X		<ul style="list-style-type: none"> • Se identifican costos y riesgos en la infraestructura de acuerdo a las modificaciones que requiera el negocio y al estudio de factibilidad realizado en el Departamento de Sistemas. Sin embargo no se cuenta con documentación formal.

<p>Plan para adquisición de hardware y software de tecnología de información.</p> <ul style="list-style-type: none"> • Se planean el impacto logístico y ambiental de las adquisiciones tecnológicas. • Suelen satisfacer las necesidades identificadas en el plan de infraestructura tecnológica y si éstos son aprobados apropiadamente. 		<p>X</p>	<ul style="list-style-type: none"> • El análisis del impacto de las adquisiciones tecnológicas se realiza de acuerdo a la experiencia del Jefe del Departamento de Sistemas. No se basa en una metodología específica, sino en estándares propios. • La infraestructura satisface las necesidades identificadas, pero éstas solo se encuentran reflejadas en el plan operativo anual.
<p>Plan de infraestructura tecnológica.</p> <ul style="list-style-type: none"> • El plan de infraestructura tecnológica está siendo comparado con los planes de tecnología de información a largo y corto plazo. 		<p>X</p>	<ul style="list-style-type: none"> • No existe un plan de infraestructura ni de tecnologías de la información. Estos datos están reflejados en el plan operativo anual.
<p>Estándares de tecnología.</p> <ul style="list-style-type: none"> • La necesidad de evaluar sistemáticamente el plan tecnológico por razones de contingencia. • Estándares para los componentes tecnológicos descritos en el plan de infraestructura tecnológica. 		<p>X</p>	<ul style="list-style-type: none"> • No existe un plan tecnológico, solo el plan operativo anual del Departamento de Sistemas. • No existen estándares para los componentes tecnológicos.

Tabla 8 Directrices de auditoría de APO04.

4.4.2.6 APO07 GESTIONAR LOS RECURSOS HUMANOS.

Entradas	Si	Parcialmente	No	Observaciones
<p>Roles y responsabilidades de la Gerencia de Planificación.</p> <ul style="list-style-type: none"> • Control del cumplimiento de roles y responsabilidades. • Asignación de un oficial de seguridad para formulación de políticas y procedimientos de control interno y de seguridad. 		X		<ul style="list-style-type: none"> • Existe control de cumplimiento de los roles y responsabilidades mediante el formato de desempeño emitido por el Departamento de Talento Humano, además del control que lleva el Jefe del departamento de Sistemas sobre las tareas asignadas. • No se tiene un oficial de seguridad para implantar políticas de control interno y seguridad. Solo existen disposiciones gerenciales que hacen referencia al control y seguridad.
<p>Organigrama organizacional que muestre la relación entre TI y otras funciones.</p> <ul style="list-style-type: none"> • Segregación de funciones. 		X		<ul style="list-style-type: none"> • Las funciones para los roles de Jefe del Departamento de Sistemas y Operador de Sistemas y Soporte de usuarios están definidas. Sin embargo, en la práctica estas funciones son realizadas por todos los roles de acuerdo a la disponibilidad de tiempo.
<p>Políticas y procedimientos relacionados con la organización y las relaciones de TI.</p>		X		<ul style="list-style-type: none"> • No existen procesos documentados para determinar la efectividad y aceptación de TI. Sin embargo, los indicadores de desempeño son identificados

<ul style="list-style-type: none"> • Procesos e indicadores de desempeño para determinar la efectividad y aceptación de TI. • Procesos de conciencia, comprensión y habilidad para resolución de problemas de administración, seguridad y control interno. • Procedimientos aplicables a los contratos de TI, adecuados y consistentes con las políticas de adquisición de la organización. • Procesos para coordinar, comunicar y documentar los intereses dentro y fuera de la estructura organizacional de TI. 			<p>internamente de acuerdo a la experiencia del Jefe del Departamento de Sistemas.</p> <ul style="list-style-type: none"> • No existen procesos documentados de concientización, comprensión y habilidad para resolución de problemas de administración de información, seguridad y control interno. • No se tienen procedimientos documentados para realizar contratos. Los contratos dependen de cada proveedor y de los términos que se acuerden entre el cliente y el proveedor. • No existe un proceso definido, aunque la Gerencia emite comunicaciones y disposiciones sobre las resoluciones tomadas a nivel organizacional y tecnológico.
<p>Políticas y procedimientos utilizados para determinar los requerimientos de asignación de personal de TI.</p>		<p>X</p>	<ul style="list-style-type: none"> • No existen políticas o procedimientos en este aspecto, aunque el Jefe del Departamento de Sistemas puede sugerir la contratación de más personal para cubrir con las necesidades de la organización.
<p>Organigrama organizacional de TI.</p>	<p>X</p>		<ul style="list-style-type: none"> • Se evalúa y se hacen modificaciones del organigrama de acuerdo a actualizaciones requeridas.

<ul style="list-style-type: none"> • Políticas que consideran la necesidad de evaluar y modificar la estructura organizacional para satisfacer objetivos y circunstancias cambiantes. 			
<p>Roles y responsabilidades de TI.</p> <ul style="list-style-type: none"> • Determinación de roles y responsabilidades con respecto a sistemas de información, control interno y seguridad, y procesos claves. 		X	<ul style="list-style-type: none"> • Están definidas las funciones para cada rol en el Departamento de Sistemas, pero los procesos claves no tienen asignados responsables ya que no se tienen definidos procesos formales dentro de la Cooperativa.
<p>Descripción de los puestos claves de TI.</p> <ul style="list-style-type: none"> • Existencia de evaluaciones y reevaluaciones de las descripciones de los puestos de trabajo de TI. 	X		<ul style="list-style-type: none"> • Al menos una vez al año se hacen evaluaciones de cada puesto de trabajo descrito en el Manual de Perfiles.
<p>Políticas y procedimientos relacionados con la administración de recursos humanos.</p> <ul style="list-style-type: none"> • Se da reforzamiento a la política de no interrumpir los días de descanso. • Si el proceso de retiro del personal de seguridad de la organización es adecuado. 		X	<ul style="list-style-type: none"> • Los días de vacaciones solamente se gestionan teniendo en cuenta el reglamento interno de trabajo y de acuerdo con el plan anual de vacaciones elaborado por el Departamento de Talento Humano. • En el Departamento de Talento Humano se toman medidas para cumplir con las leyes y regulaciones aplicables.

<ul style="list-style-type: none"> • Los procesos de terminación de contrato y cambio de puesto aseguran la protección de los recursos de la organización. • Las políticas y procedimientos de recursos humanos concuerdan con leyes y regulaciones aplicables. 				<ul style="list-style-type: none"> • En el caso que una persona deje de pertenecer a la organización, el Departamento de Sistemas tiene la responsabilidad de eliminar la cuenta del usuario correspondiente para evitar que ingrese al sistema una vez que ya no sea trabajador de la Cooperativa.
<p>Espedientes del personal y archivos de puestos de trabajo para posiciones seleccionadas.</p> <ul style="list-style-type: none"> • Criterios para reclutamiento y selección de personal. • Especificaciones de habilidades y conocimientos requeridos. 	X			<ul style="list-style-type: none"> • El procedimiento que se realiza para reclutamiento y selección de personal es dirigido estrictamente por el Departamento de Talento Humano y es aceptado y conocido por el resto del personal de la Cooperativa.

Tabla 9 Directrices de auditoría de APO07.

4.4.2.7 APO11 GESTIONAR LA CALIDAD.

Entradas	Si	Parcialmente	No	Observaciones
<p>Políticas y procedimientos relacionados con el aseguramiento de la calidad.</p> <ul style="list-style-type: none"> • Identificación y definición de la calidad de roles y responsabilidades. 		X		<ul style="list-style-type: none"> • No se identifica ni define la calidad de roles y responsabilidades. • No existe un procedimiento para evaluar la calidad, aunque internamente el Departamento de Sistemas realiza pruebas de funcionamiento y de aceptación

<ul style="list-style-type: none"> • Programación de recursos, cumplimiento de las pruebas, aprobación del aseguramiento de la calidad antes que se implementen nuevos sistemas o se produzcan cambios. 			<p>antes de la entrega de un equipo o sistema al usuario final antes del pase a producción.</p>
--	--	--	---

Tabla 10 Directrices de auditoría de APO11.

4.4.2.8 APO12 GESTIONAR EL RIESGO.

Entradas	Si	Parcialmente	No	Observaciones
<p>Políticas y procedimientos relacionados con la evaluación de riesgos.</p> <ul style="list-style-type: none"> • Marcos referenciales para la evaluación sistemática de riesgos. • Evaluación actualizada regular de riesgos a nivel global y específico de sistemas. • Procedimientos de evaluación de riesgo que toman en cuenta factores internos y externos, y consideran resultados de auditorías, inspecciones e incidentes identificados. 			X	<ul style="list-style-type: none"> • No existen marcos referenciales para la evaluación del riesgo. Únicamente se cuenta con la experiencia del personal de TI y se realiza internamente en el Departamento de Sistemas. • No se realiza una evaluación regular de riesgos a nivel global, aunque el análisis de riesgos de TI se realiza en cada proyecto de manera informal. • No se cuenta con un procedimiento de evaluación de riesgos. Cada evaluación del riesgo se hace de acuerdo a los nuevos requerimientos del negocio que serán implementados.

<ul style="list-style-type: none"> • Balance entre las medidas de detección, prevención, corrección y recuperación utilizadas. • Procedimientos formales para comunicar el propósito de la medición de los controles. 			<ul style="list-style-type: none"> • No se tiene en cuenta un balance entre las medidas de detección, prevención, corrección y recuperación existentes. • No existen procedimientos formales para comunicar el propósito de la medición de controles.
<p>Documentos de evaluación de riesgos del negocio.</p> <p>Incluyen los objetivos de la organización en el proceso de identificación de riesgos.</p>		X	<ul style="list-style-type: none"> • No existe documentación de evaluación de riesgos, esto se maneja internamente en el Departamento de Sistemas. Esto se maneja en el Plan Operativo de la Cooperativa.
<p>Documentos de evaluación de riesgos operativos.</p> <p>Procedimientos para monitoreo y mejoramiento continuo de la evaluación de riesgos y procesos para la creación de controles que mitiguen los riesgos.</p>		X	
<p>Detalles de la base sobre la que se miden los riesgos y la exposición a los riesgos.</p>			<ul style="list-style-type: none"> • No existe una metodología de riesgos, aunque se realiza la identificación de riesgos a nivel interno y de manera informal, estos resultados son comunicados a la Gerencia mediante oficios o reuniones informales.

<p>Incluyen descripción de la metodología de riesgos, identificación de la exposición significativa.</p> <p>Se usan técnicas de probabilidad, frecuencia y análisis de amenazas en la identificación de riesgos o cañculos y otros métodos en la medición de riesgos, amenazas y exposiciones.</p>			<ul style="list-style-type: none"> No se utilizan técnicas probabilidad, solo se definen estimaciones con el establecimiento de escenarios y posibles pérdidas económicas en el establecimiento de riesgos operativos.
<p>Expedientes para personal seleccionado de evaluación de riesgos.</p>		<p>X</p>	<ul style="list-style-type: none"> No hay definida un área que se encargue de la evaluación de riesgos, por lo que el personal responsable de esta tarea es el asignado por el Departamento de Sistemas.
<p>Políticas de seguros que cubren el riesgo residual.</p> <p>Se toma en cuenta la política organizacional, identificación y medición de riesgos, incertidumbre inherente al enfoque de la evaluación de riesgos, el costo y la efectividad de implementar salvaguardas y controles.</p>		<p>X</p>	<ul style="list-style-type: none"> Solo existen seguros para riesgos que puedan producir pérdidas.
<p>Resultados de las opiniones de expertos o grupos especializados.</p>		<p>X</p>	<ul style="list-style-type: none"> Se realizan internamente.

Consulta de las bases de datos de administración de riesgos.			X	<ul style="list-style-type: none"> • No existe una base da datos de administración de riesgos.
--	--	--	----------	---

Tabla 11 Directrices de auditoría de APO12.

4.4.2.9 SÍNTESIS GLOBAL DEL DOMINIO APO

La Cooperativa de Ahorro y Crédito Nueva Esperanza en un nivel global está consciente de la importancia de contar con procesos documentados para el manejo de tecnologías de información a pesar que no tienen estos procesos definidos formalmente, por lo que actualmente se realizan de manera repetitiva e intuitiva. No se cuenta con documentación que respalde las funciones realizadas por el Departamento de Sistemas, lo que impide una comunicación transparente y directa con el resto de la Organización.

Podemos decir que la planificación estratégica de TI se encuentra alineada con la de la Institución, por lo que se definen objetivos claros a corto y largo plazo, están sujetos a actualizaciones teniendo en cuenta la aparición de nuevos requerimientos del negocio, regulaciones, aspectos legales y tecnologías emergentes en la industria.

Es importante mencionar que la gestión del Departamento de Talento Humano de TI establece una organización del Departamento de Sistemas anual, y sus funciones son sensibles a cambios. También el Jefe del Departamento de Sistemas cumple con sus funciones teniendo en cuenta la experiencia, práctica y habilidades adquiridas anteriormente.

En cuanto al análisis de riesgos tecnológicos se puede concluir que se realiza internamente por el Jefe del Departamento de Sistemas y no cuenta con un proceso documentado, pero sigue una política de comunicación directa con la Gerencia. Esto lo realiza de acuerdo a su experiencia y conocimientos adquiridos anteriormente. Es importante mencionar que esta responsabilidad no está en sus funciones definidas en el Manual de Perfiles de la Cooperativa.

4.4.2 CONSTRUIR, ADQUIRIR E IMPLEMENTAR (BAI)

4.4.2.1 BAI02 GESTIONAR LA DEFINICIÓN DE REQUISITOS.

Entradas	Si	Parcialmente	No	Observaciones
<p>Políticas y procedimientos relacionados con el ciclo de vida del desarrollo de sistemas y con la adquisición de software.</p> <ul style="list-style-type: none"> • Se ha desarrollado e implementado un enfoque de adquisición central, que describa un conjunto común de procedimientos y estándares para ser seguidos en la adquisición de hardware, software y servicios de TI. • Existe documentación de los requerimientos de usuarios satisfechos por el sistema existente o que serán satisfechos por nuevo sistema propuesto, que son revisados y aprobados. • Existe documentación de los requerimientos operativos y funcionales de la solución o soluciones alternativas que 		X		<ul style="list-style-type: none"> • No existe un Manual de adquisiciones en el que se describan los procedimientos para adquirir cualquier recurso que requiera la empresa. • Existe una solicitud de requerimientos que los usuarios utilizan para manifestar sus necesidades al Departamento de Sistemas con respecto a hardware y software. Estas solicitudes son analizadas por el Jefe del Departamento de Sistemas para darle solución lo antes posible. En cuanto se satisface la necesidad, el usuario firma un documento de conformidad. • En el Manual de Adquisición se establece que deben existir al menos 3 alternativas para la adquisición de soluciones tecnológicas, las cuales son analizadas y aprobadas por el Consejo de Administración. • Se realiza un análisis de factibilidad teniendo en cuenta la experiencia del Jefe del departamento de Sistemas, cuyos resultados se comunican a la

<p>incluyen aspectos como el desempeño, seguridad, confiabilidad, compatibilidad.</p> <ul style="list-style-type: none"> • Las alternativas para la adquisición de los productos de software estan claramente definidos y que se puedan adquirir en el mercado, internamente desarrollados, a través de contratos o mejorar el software existente. • Existe un estudio de factibilidad técnica para cada alternativa con el fin de satisfacer los requerimientos establecidos por el usuario. • En cada proyecto de desarrollo, modificación o implementación de sistemas, se lleva a cabo un análisis de los costos y beneficios. • Se toma en cuenta el modelo de datos de la empresa mientras se identifica y analiza la factibilidad de las soluciones. • Se prepara y documenta un análisis de las amenazas a la seguridad, de las debilidades y los impactos potenciales y las 			<p>Gerencia y faciliten la toma de decisiones con relación a la adquisición de nuevas soluciones.</p> <ul style="list-style-type: none"> • Se realiza un análisis de costo y beneficio para implementaciones de soluciones tecnológicas, sin embargo es un proceso se realiza internamente en el Departamento de Sistemas. • No existe un modelo d edatos definido para la identificación de soluciones tecnológicas. • Se realiza un análisis de riesgos que es manejado por el Jefe de Sistemas internamente en el departamento, aunque esta función no es responsabilidad asignada a su cargo. • No se realizan controles ni auditorías. Solo existen documentos de pases a producción cuando se realiza una actualización en el sistema. • No existe un plan de aceptación para tecnología con los proveedores, solamente se firma un contrato con los mismos.
---	--	--	---

<p>salvaguardas factibles de seguridad y control interno para reducir o eliminar el riesgo identificado.</p> <ul style="list-style-type: none"> • Se requieren controles y pistas de auditoría apropiados para ser aplicados en todos los sistemas modificados o nuevos propuestos durante la fase de diseño del proyecto. 				
---	--	--	--	--

Tabla 12 Directrices de auditoría de BAI02.

4.4.2.2 BAI03 GESTIONAR LA IDENTIFICACIÓN Y CONSTRUCCIÓN DE SOLUCIONES

Entradas	Si	Parcialmente	No	Observaciones
<p>Políticas y procedimientos relacionados con la metodología del ciclo de vida del desarrollo de sistemas.</p> <ul style="list-style-type: none"> • Existe una metodología del ciclo de vida de desarrollo de sistemas de la organización que se aplica tanto para el desarrollo de nuevos sistemas como para sus modificaciones. • Las especificaciones de diseño son aprobadas por la Gerencia. 		X		<ul style="list-style-type: none"> • Sí existe una metodología que rige el ciclo de vida del desarrollo de sistemas que consta de las siguientes fases: recolección de requerimientos, desarrollo, pruebas y Aprobación que está registrada en el Documento de Segmento 4. • El usuario final puede interactuar con la especificación de diseño durante todo el ciclo de vida de desarrollo del sistema. • Las especificaciones son aprobadas por Auditoría Interna, Gerencia General, Jefe de Sistemas y finalmente por el usuario final.

<ul style="list-style-type: none"> • Se especifican los mecanismos adecuados para la captura y documentación de requerimientos para cada proyecto nuevo o modificado. • Existe el software de aplicación que es aprobado de acuerdo con el plan de pruebas del proyecto y los estándares establecidos. • Se realizan manuales adecuados de soporte y referencia para usuarios como parte del proceso de desarrollo o modificación de cada sistema. 			<ul style="list-style-type: none"> • Se utiliza un formato de solicitud de requerimientos donde se registra: origen, área, departamento, prioridad, detalle del requerimiento, persona que lo solicita, comentario, aprobado por, fecha de inicio, fecha de finalización y responsable, registrado en el Documento de Segmento 4. • No existe un plan de pruebas del software de aplicación, solamente las aprobaciones dentro del ciclo de vida de desarrollo por parte del usuario final y Auditoría Interna. • El ciclo de vida de desarrollo del software concluye con la realización de manuales de usuario. En el caso de realizar una modificación, se realizan manuales con los cambios realizados.
<p>Políticas y procedimientos relacionados con la adquisición, implementación y mantenimiento de hardware y software.</p> <ul style="list-style-type: none"> • Existen políticas y procedimientos para el mantenimiento preventivo de hardware para reducir la frecuencia y el impacto de las fallas de desempeño. 		<p>X</p>	<ul style="list-style-type: none"> • Existe un procedimiento de mantenimiento preventivo que se realiza regularmente. • No existe un plan de evaluación para el nuevo hardware y software, aunque para las soluciones de software sí existe un ambiente de pruebas antes de su pase a producción. • No existe la amenaza de pérdidas de datos ya que se tienen respaldos de la información sensible, de igual

<ul style="list-style-type: none"> • Existe un plan de evaluación formal para el nuevo hardware y software en cuanto al impacto sobre el desempeño global del sistema. • La preparación, instalación y mantenimiento del software del sistema no amenaza la seguridad de los datos y programas almacenados en el sistema. 				forma los sistemas se prueban antes de pasarlos al ambiente de producción.
Documentos sobre vendedores de hardware y software.	X			
Contratos de mantenimiento o acuerdos de arrendamiento con opción de compra de hardware y software	X			

Tabla 13 Directrices de auditoría de BAI03.

4.4.2.3 BAI05 GESTIONAR LA FACILITACIÓN DEL CAMBIO ORGANIZATIVO.

Entradas	Si	Parcialmente	No	Observaciones
Los procedimientos de operación y usuarios antes de la implementación, durante las		X		<ul style="list-style-type: none"> • No tienen materiales de capacitación que abarquen todas las funciones del sistema, unicamente para las que son consideradas fundamentales por parte del Jefe del Departamento de Sistemas.

<p>pruebas de aceptación son para asegurarse de que son completos, exactos y utilizables.</p> <ul style="list-style-type: none"> • Se crean las instrucciones necesarias para el usuario, documentación, procedimientos y materiales de capacitación de manera oportuna para permitir el uso eficiente y eficaz del nuevo sistema. • Se cuenta con documentación informativa y comprensible para el usuario final y los materiales de referencia deben estar diseñados para todos los niveles de especialización, escrito en lenguaje sencillo y accesible. 			<ul style="list-style-type: none"> • La documentación se desarrolla en un lenguaje comprensible para los usuarios y es accesible a los involucrados que la necesiten. • En el desarrollo de la documentación de soporte al usuario únicamente intervienen las personas que hicieron las actualizaciones en el sistema.
<p>Funciones de gestión, procedimientos de seguridad y control, y requisitos de capacitación.</p> <p>Se realiza capacitación a los usuarios finales sobre cómo utilizar el sistema de forma eficaz.</p> <p>Recopilar información periódica de los usuarios finales sobre la modificación de la</p>		<p>X</p>	<ul style="list-style-type: none"> • En el manual de operaciones se definen las funciones que debe realizar cada usuario en el sistema. En el caso de realizar cambios al sistema, se actualizan los manuales de los usuario o se realiza una capacitación informal. • No existe recopilación periódica de usuarios finales.

documentación, los procedimientos y la capacitación.				
--	--	--	--	--

Tabla 14 Directrices de auditoría de BAI05.

4.4.2.4 SÍNTESIS GLOBAL DEL DOMINIO BAI

En la Cooperativa de Ahorro y Crédito Nueva Esperanza existe la concientización sobre la necesidad de construir, adquirir e implementar soluciones tecnológicas que contribuyan con el cumplimiento de los objetivos de la Entidad. Sin embargo, hay que señalar que no existe un proceso específico de adquisición de recursos y soluciones de TI ni existe un Manual de Adquisiciones que se enfoque en aspectos globales del negocio.

En estos momentos el Jefe del Departamento de Sistemas es el responsable de identificar y mantener las soluciones automatizadas, mientras que la adquisición depende de la Gerencia, donde el Departamento de Sistema solo se encarga de proporcionar un tema de proveedores basado en un análisis de costo-beneficio y de riesgos tecnológicos que es analizado por el Comité Ejecutivo y finalmente aprobado por la Gerencia.

En cuanto al mantenimiento de recursos de TI, se realiza de manera preventiva y correctiva en periodos regulares, sin un proceso documentado. Para esto no se rige por ninguna metodología, aunque se tiene en cuenta las habilidades y experiencia del personal de Departamento de Sistemas.

También existe la documentación referente a manuales de usuarios proporcionados por el proveedor del Sistema Financiero, mientras que la producción de la documentación para este tipo de documentación no está estandarizada y solo existe en casos considerados como necesarios por el Jefe del Departamento de Sistemas. Cabe señalar que el desarrollo de la documentación no está contemplado dentro de un plan, sino que se realiza de acuerdo a requerimientos del negocio y usuarios.

4.4.3 ENTREGA, SERVICIO Y SOPORTE (DSS)

4.4.4.1 DSS04 GESTIONAR LA CONTINUIDAD DEL SERVICIO

Entradas	Si	Parcialmente	No	Observaciones
<p>Políticas y procedimientos relacionados con los procesos de planificación de recuperación/continuidad.</p> <ul style="list-style-type: none"> • Una lista de los recursos de sistema que requieren alternativas como hardware, software, centro de cómputo de respaldo, archivos de datos, manuales de usuarios, etc. • Escenarios de desastres varios y respuesta a cada uno para llevar a cabo una ejecución paso a paso. Entrenamiento sobre las funciones individuales y del equipo en el plan de continuidad. • Requerimientos de la agencia reguladora con respecto a la planificación de continuidad. 		<p>X</p>		<ul style="list-style-type: none"> • No existen políticas ni procedimientos documentados de TI para garantizar la continuidad de los servicios, actualmente se están desarrollando. Actualmente se encuentra en proceso el plan de contingencia a nivel de departamento. • Existe un inventario de los recursos de TI que se actualiza semestralmente. • Actualmente no existen escenarios de desastres ni respuestas a cada uno de ellos, aunque se está contratando a un proveedor de respaldos para evitar fallas de comunicación e insatisfacción a los clientes. • No se utilizan metodologías para priorizar las aplicaciones para la recuperación. • Actualmente se encuentran en la implementación de un plan de contingencias que garantice la continuidad de los servicios.

<ul style="list-style-type: none"> • Priorización de aplicaciones con respecto a los tiempos de recuperación. 			
<p>Políticas y procedimientos de la función de servicios de información relacionados con un marco referencial de continuidad, plan, filosofía, estrategia, plan de pruebas, respaldos, así como entrenamiento de recuperación de desastres.</p> <ul style="list-style-type: none"> • Se tiene un marco de trabajo referencial de continuidad y de un plan para la función de servicios de información y áreas dependientes de los recursos de sistemas de información. • Roles y responsabilidades específicas para la planificación de continuidad, con pruebas, mantenimiento y requerimientos de actualización. 		X	<ul style="list-style-type: none"> • La Cooperativa no cuenta con un marco de trabajo formal para la continuidad de todos los servicios de TI, aunque el Departamento de Sistemas se encarga de definir alternativas para posibles casos de emergencia relacionadas a servicios fundamentales para el negocio y evitar así posibles insatisfacciones de los socios. • La responsabilidad de definir la continuidad de los servicios de TI no está asignada a un rol en específico aunque es realizada informalmente por el Jefe del Departamento de Sistemas.
<p>Contrato de los proveedores que dan soporte a los servicios de continuidad.</p>		X	<ul style="list-style-type: none"> • En los contratos con proveedores se establecen cláusulas para que ellos sean responsables de garantizar la continuidad de los servicios provistos.

<ul style="list-style-type: none"> • Acuerdos de contrato formal con los proveedores de servicios en cuanto a la recuperación de información. • Funciones administrativas para comunicar y proporcionar servicios de soporte como beneficios, nómina, comunicación externa, seguimiento de costos, etc. 			<ul style="list-style-type: none"> • No está especificada la responsabilidad de recuperación para los servicios de terceros. • En los acuerdos de niveles de servicio no se definen funciones administrativas para los eventos de recuperación.
---	--	--	---

Tabla 15 Directrices de auditoría de DSS04.

4.4.4.2 DSS05 -GESTIONAR SERVICIOS DE SEGURIDAD.

Entradas	Si	Parcialmente	No	Observaciones
<p>Políticas y procedimientos para la Cooperativa referentes a la seguridad y acceso a los sistemas.</p> <ul style="list-style-type: none"> • Se tiene un plan de seguridad estratégico que proporcione dirección y control sobre la seguridad de sistemas y recursos de TI. • Se tiene una organización de seguridad responsable de asegurar el acceso adecuado a los recursos del sistema. 		X		<ul style="list-style-type: none"> • La Cooperativa cuenta con políticas de seguridad de acceso a nivel general que están definidas en el reglamento de seguridad, sin embargo en lo que se refiere al área de sistemas, no existe un plan de seguridad específico, en su lugar existen medidas implementadas por el Jefe del Departamento de Sistemas. • Actualmente no existe una organización de seguridad responsable, esta función es delegada al Departamento de Sistemas.

<ul style="list-style-type: none"> • Entrenamiento de los empleados sobre conocimientos y conciencia relacionados con la seguridad. 			<ul style="list-style-type: none"> • Los empleados tienen conocimientos sobre aspectos fundamentales de seguridad de TI pero no cuentan con un entrenamiento sistemático de este tema.
<p>Procedimientos y políticas de TI relacionadas con seguridad y acceso a la información.</p> <ul style="list-style-type: none"> • Se tienen los datos clasificados en operaciones que indiquen que cada recurso tiene un propietario responsable de su seguridad. <p>Existen perfiles de usuarios y se hacen revisiones regulares de los mismos por parte de la administración.</p> <ul style="list-style-type: none"> • Se tienen reportes de fallas de seguridad y procedimientos formales de solución. • Se tienen mecanismos de autenticidad en uso con número de sesiones concurrentes limitadas, así como políticas de contraseñas. • Se utilizan rutas confiables para transmitir información sensible no encriptada. 		<p>X</p>	<ul style="list-style-type: none"> • El Sistema Financiero es encargado de realizar y controlar la clasificación de datos, quien garantiza que exista acceso restringido a la información de acuerdo a los perfiles de usuarios. • El Departamento de Sistemas define perfiles de usuarios de acuerdo a la responsabilidad del personal y están sujetos a revisiones y actualizaciones periódicas. • El Sistema Financiero se encarga de relajar reportes de fallas de seguridad, aunque estos no cuentan con procedimientos formales de solución. • No se utilizan estándares para la administración de llaves de seguridad. • Existen políticas de contraseñas para el Sistema Financiero que son generadas automáticamente por un módulo de administración del propio sistema. • La transmisión de información sensible se realiza mediante la red interna de la Cooperativa, a la que

<ul style="list-style-type: none"> • Se establecen medidas de control para prevenir y detectar virus. 			<p>solo tiene acceso el personal de la empresa y cuenta con seguridad para no permitir el ingreso de intrusos.</p> <ul style="list-style-type: none"> • El Departamento de Sistemas se encarga de mantener antivirus actualizados en las máquinas, así como del bloqueo de puertos USB y restricción a sitios web no relacionados con las actividades laborales.
<p>Políticas y procedimientos generales sobre controles y conciencia de seguridad.</p> <ul style="list-style-type: none"> • Los nuevos empleados tienen conocimiento de la responsabilidad de seguridad y control en cuanto al uso de recursos de TI. • Existe disponibilidad de oportunidades y frecuencia de entrenamiento, considerando la asistencia de los empleados. 		<p>X</p>	<ul style="list-style-type: none"> • Se transmite a los empleados las normas de seguridad establecidas en el reglamento interno, aunque no están definidas medidas de seguridad específicamente para los recursos de TI. • Se planifica un cronograma de cursos generales y específicos por áreas para la capacitación del personal.
<p>Políticas y procedimientos organizacionales relacionados con la administración de base de datos.</p> <ul style="list-style-type: none"> • Proceso de autorización de documentos fuente. 		<p>X</p>	<ul style="list-style-type: none"> • No se realiza un procedimiento para la administración de los datos, simplemente se debe solicitar autorización para acceder a los documentos dependiendo del nivel de confidencialidad.

<ul style="list-style-type: none"> • Procesos de recolección, seguimiento y transmisión de datos. 			<ul style="list-style-type: none"> • Los procesos de recolección, seguimiento y transmisión de datos están especificados en el manual de operaciones de cada cargo.
--	--	--	--

Tabla 16 Gestionar servicios de seguridad de DSS05.

4.4.4.3 SÍNTESIS GLOBAL DEL DOMINIO DSS

En la Cooperativa de Ahorro y Crédito Nueva Esperanza existe conciencia de la necesidad de gestionar la entrega y soporte de los servicios de TI, ya que de estos dependen en gran medida el cumplimiento de sus objetivos, así como la satisfacción de los clientes.

Para la gestión de este dominio se toman medidas como establecer la responsabilidad de revisión y firma de los contratos a la Gerencia, Comité Ejecutivo y Asesoría legal para la parte operativa y legal.

No existe un acuerdo de niveles de servicio, en su lugar la Cooperativa dispone de un contrato escrito en el que se reflejan las condiciones del servicio prestado por el proveedor, centradas en el negocio y no en aspectos tecnológicos, y tampoco se especifican métricas para evaluar el desempeño del servicio.

El Departamento de Sistemas dispone de un inventario de todos los componentes de TI pero en este no se clasifican según su importancia para el negocio ni cuenta con un plan de capacidad que permita a la Gerencia conocer el desempeño actual y futuro de los componentes de TI. Solo cuentan con un análisis de costo-beneficio, factibilidad y riesgos, que es realizado por el Jefe de Sistemas, de acuerdo a su experiencia y conocimientos, con el fin de comunicar a la Gerencia los nuevos requerimientos de capacidad y desempeño que la Cooperativa debería adquirir para cubrir con las exigencias del negocio.

A pesar que existen políticas de continuidad de los servicios de TI no se encuentran documentadas ni integradas en un plan de continuidad. Es por esto que el Departamento de Sistemas es el encargado de ejecutar las medidas de respaldo de información, comunicar a los proveedores de problemas relacionados con sus servicios, resolver inconvenientes con el Sistema Financiero, etc. En el caso que se presenten problemas de identificación de usuarios, existe un formato de solicitud de requerimientos que permite al Departamento de Sistemas darle solución oportunamente.

4.4.4 SUPERVISAR, EVALUAR Y VALORAR (MEA)

4.4.4.1 MEA01 SUPERVISAR, EVALUAR Y VALORAR EL RENDIMIENTO Y LA CONFORMIDAD

Entradas	Si	Parcialmente	No	Observaciones
<p>Políticas y procedimientos para establecer prioridades y asignar responsabilidades en el monitoreo del desempeño ya la capacidad de presentación de servicios de TI.</p> <ul style="list-style-type: none"> Existen objetivos claros para llevar a cabo revisiones periódicas e iniciación de acciones correctivas. 		X		<ul style="list-style-type: none"> Existen revisiones periódicas y acciones correctivas basadas en medidas establecidas por el Jefe del Departamento de Sistemas y son realizadas periódicamente. Aunque no existe capacitación para la medición de desempeño.
<p>Reportes de costo-beneficio, desempeño de proyectos y procesos, satisfacción de usuarios.</p> <ul style="list-style-type: none"> Existe la comunicación de reportes de desempeño periódicos de los procesos para elaborar reportes gerenciales que pueden ser utilizados para decisiones estratégicas y son discutidos en reuniones de la Gerencia analizando la contribución de TI al negocio. 		X		<ul style="list-style-type: none"> Los porcentajes del procesamiento de transacciones y el costo del recurso humano son indicadores claves de rendimiento que permiten a la Gerencia conocer el impacto económico de la interrupción de los servicios y tomar decisiones oportunas. No existe la identificación de procesos sobresalientes, por lo que no existe un registro de la cantidad de deficiencias de los mismos. El Jefe del Departamento de Sistemas propone a la Gerencia las mejoras del desempeño de TI

<ul style="list-style-type: none"> • Acciones de mejora impulsadas por las actividades de monitoreo. 				respaldadas por un informe de costo-beneficio y factibilidad, para su posterior análisis y aprobación.
<ul style="list-style-type: none"> • Reportes sobre el cumplimiento de las actividades de TI respecto a requerimientos legales y regulatorios externos. • Existe una falta de identificación de problemas relacionados con la informática. • Establecer un sistema de control de TI que está ligado a las estrategias del negocio y facilita el control eficaz de las TI. 				<ul style="list-style-type: none"> • Los problemas se identifican durante el periodo de desarrollo del plan estratégico y se solucionan para que estén de acorde a la alineación con el negocio. • No existe un sistema de control de TI ligado a las estrategias del negocio, sin embargo se realizan actividades por parte del Jefe del Departamento de Sistemas en base a su experiencia.

Tabla 17 Directrices de auditoría de MEA01.

4.4.4.2 MEA02 -SUPERVISAR, EVALUAR Y VALORAR EL SISTEMA DE CONTROL INTERNO.

Entradas	Si	Parcialmente	No	Observaciones
<p>Políticas, procesos y procedimientos para establecer controles internos de TI que son reportados a la Gerencia.</p> <ul style="list-style-type: none"> • Existe un sistema de control interno documentado que emite reportes de anomalías, y se determina acciones correctivas en base a riesgos de seguridad 		X		<ul style="list-style-type: none"> • No existe un sistema de control interno, por lo que no existen actualizaciones correspondientes. Actualmente el control interno se lleva a cabo mediante el uso de herramientas de ofimática. • No hay políticas definidas que exijan la utilización de una metodología, sin embargo por la experiencia del Auditor Interno se han estado utilizando procesos de COSO para el control interno, aunque no se está

<p>informática y cumplimiento del reglamento.</p> <ul style="list-style-type: none"> • El sistema de control interno está sujeto a modificaciones de acuerdo al entorno de control de la Institución. • Está implementada una política basada en estándares y prácticas aceptadas en la industria, asociada a actividades de seguimiento y evaluación. • Hay asignado un responsable para la definición formal de los controles internos. 			<p>aplicando específicamente al Departamento de Sistemas.</p> <ul style="list-style-type: none"> • En estos momentos el responsable de realizar los controles internos es el Departamento de Auditoría Interna.
<p>Reportes de efectividad de controles internos de TI.</p> <p>Están documentadas las debilidades identificadas para la mejora continua.</p> <p>Existen requisitos de control interno establecidos en los contratos con los proveedores.</p>		<p>X</p>	<ul style="list-style-type: none"> • No existe documentación ni se tienen identificadas las debilidades que puedan afectar la mejora continua del control. • Con relación a los proveedores, solamente existe control del cumplimiento de los contratos.

Tabla 18 Directrices de auditoría de MEA02.

4.4.4.3 MEA03. SUPERVISAR, EVALUAR Y VALORAR LA CONFORMIDAD CON LOS REQUERIMIENTOS EXTERNOS.

Entradas	Si	Parcialmente	No	Observaciones
<p>Reporte sobre el cumplimiento de las actividades de TI con los requerimientos legales y regulatorios.</p> <ul style="list-style-type: none"> • Documentación de publicación de una nueva ley o regulación, lo que implica una revisión de su cumplimiento. • Presentación de informes de las revisiones del cumplimiento. • Evaluar el impacto de los requisitos legales y reglamentarios en los contratos relacionados con las operaciones de TI, proveedores de servicios de terceros y socios comerciales. • Mantener un registro actualizado de todos los requisitos legales, su impacto y acciones requeridas. 		X		<ul style="list-style-type: none"> • Cuando se realiza una actualización en las leyes, los Organismos de Control comunican el cambio mediante reportes a la Institución para que se hagan las respectivas modificaciones según sea el caso. • Los Organismos de Control teniendo en cuenta las condiciones legales y regulatorias, emiten informes periódicos sobre las revisiones y sus resultados. • No se realiza una evaluación del impacto sobre los requisitos legales y reglamentarios, solo se controla que se cumpla con las leyes relacionadas con TI. • El registro de todos los requisitos legales, reglamentarios y contractuales es realizado por los Organismos de Control.

Tabla 19 Directrices de auditoría de MEA03.

4.4.4.4 SÍNTESIS GLOBAL DEL DOMINIO MEA

La Cooperativa de Ahorro y Créditos Nueva Esperanza es consciente de la necesidad de implementar un procesos de monitoreo y evaluación en el área de TI que permita conocer cómo su desempeño está apoyando los objetivos del negocio y llevar un control de todas las actividades que se realizan.

Además, reconoce la importancia de establecer un proceso definido que documente el control interno de TI para garantizar que se cumplan los objetivos del Departamento de Sistemas unido a las regulaciones establecidas por los Organismos de Control. Por lo que la Institución se encuentra en la planificación de un proceso definido para el establecimiento de control interno en el Departamento de Sistemas, siendo responsable el Departamento de Auditoría.

El cumplimiento regulatorio contractual y legal externo depende de los Organismos de Control y el Consejo de Vigilancia, de acuerdo a las leyes, reglamentos, estatutos y normas establecidas. Los informes y reportes se generan para dar a conocer la situación actual de la Institución con respecto a las actualizaciones de leyes y regulaciones y su cumplimiento.

4.5 ANÁLISIS DE LOS RESULTADOS

4.5.1 APO01 GESTIONAR EL MARCO DE GESTIÓN DE TI.

La Cooperativa cuenta con Manual de Perfiles donde están definidos los roles y responsabilidades del personal. Se tienen actas y libros correspondientes de cada sesión realizada para la toma de decisiones de la organización.

A pesar de esto no se tienen definidos procesos documentados, las actividades de cada departamento solo se basan en el reglamento general donde están definidas las políticas de la Cooperativa.

Se propone a la Cooperativa de Ahorro y Crédito Nueva Esperanza establecer un proceso documentado para llevar a cabo el registro de las actividades de cada departamento y definición de las responsabilidades de cada rol.

4.5.2 APO02 ADMINISTRAR LA ESTRATEGIA.

La Cooperativa cuenta con un Plan estratégico de TI definido como parte del plan estratégico Global de la Institución, que es conocido por todo el personal.

Sin embargo no está definido un proceso documentado para el desarrollo del Plan Estratégico de TI. En cuanto a los riesgos se puede afirmar que son identificados en base a un análisis costo-beneficio por iniciativa y experiencia del Jefe del Departamento de Sistemas, estos son comunicados a la Gerencia de manera informal, sin un proceso definido y documentado.

Por lo anterior mencionado se propone establecer una política que indique que la Gerencia debe monitorear el proceso de definición del Plan Estratégico de TI, de manera que pueda tomar decisiones basándose en este plan y en la medición de su efectividad. Así como establecer un proceso de monitoreo para asegurar la ejecución de los objetivos a corto y largo plazo. Establecer procesos documentados para determinar los recursos internos y externos para el desarrollo y operaciones de los sistemas.

4.5.3 APO03. GESTIONAR LA ARQUITECTURA EMPRESARIAL.

En la Institución se reconoce que es necesario definir la arquitectura de información, sin embargo, en la práctica este concepto está asociado a clasificar, organizar y almacenar los datos de los clientes siguiendo un proceso no definido sin procedimientos y la documentación necesaria.

Por lo que se propone establecer un proceso documentado para llevar a cabo la definición, administración y mantenimiento de la arquitectura de información de la Cooperativa basados en estándares y buenas prácticas.

Se recomienda además asignar roles y responsabilidades para definir la arquitectura de información, cuyos responsables tengan la experiencia y capacitación adecuadas, y comunicar sobre la importancia y los componentes de la arquitectura a todo el personal de la Cooperativa.

4.5.4 APO04. GESTIONAR LA INNOVACIÓN.

La gerencia de la Cooperativa reconoce la importancia de que la infraestructura tecnológica esté acorde a los requerimientos de la Institución, sin embargo, no hay definido un plan específico

para ello, solo existe como parte del plan operativo anual, donde se definen tanto componentes tecnológicos como su implementación, que es llevada a cabo con un análisis de riesgos no documentado, por el Jefe del Departamento de Sistemas. Por lo que se puede concluir que no existe un proceso documentado y una metodología para su realización.

Es por esto que se propone establecer un proceso definido para elaborar un plan específico para infraestructura tecnológica de acuerdo a los requerimientos del negocio y tecnologías necesarias.

Aplicar técnicas y estándares tecnológicos para el desarrollo de componentes de infraestructura tecnológico, así como asignar un responsable para evaluar los cambios tecnológicos con las habilidades y experiencias necesarias.

4.5.5 O07 GESTIONAR LOS RECURSOS HUMANOS.

En la Cooperativa se reconoce la importancia de alinear la gestión de recursos de TI con la planificación que se realiza en el Departamento de Sistemas.

El plan del personal de TI se establece en el plan general de Talento Humano. No se contempla rotación del personal y se basa en la experiencia del Jefe de Talento Humano, más que en estándares de la industria.

Para contratar personal de TI se toma en cuenta que el nuevo personal esté preparado para asumir las responsabilidades que satisfagan los objetivos del negocio. Si se considera necesario, se coordina una capacitación general para el personal de TI, así como para el personal de áreas determinadas relacionadas con las tecnologías de información.

Teniendo en cuenta el análisis realizado se propone realizar una reevaluación del número de personas del departamento de Sistemas, y en base a sus resultados replantar su estructura organizacional. Crear una política, procedimiento y programa de capacitación que establezca a un responsable para suplir las funciones del Jefe de Sistemas en caso de su ausencia. Además es necesario realizar evaluaciones de desempeño de acorde a estándares y mejores prácticas existentes.

4.5.6 APO11 GESTIONAR LA CALIDAD.

En la Institución no se identificó un procedimiento para evaluar la calidad, aunque internamente el Departamento de Sistemas realiza pruebas de funcionamiento y de aceptación antes de la entrega de un equipo o sistema al usuario final antes del pase a producción.

Es por ello que se recomienda definir un proceso formal donde se genere la documentación necesaria y se adopten las pautas de calidad establecidas, para llevar a cabo la evaluación de la tecnología en la Cooperativa.

4.5.7 APO12 GESTIONAR EL RIESGO.

En la Cooperativa se tiene una conciencia de la importancia de llevar a cabo una gestión de riesgos. Sin embargo, actualmente el análisis se centra en los riesgos del negocio y no se presta la debida atención a los riesgos de TI que pueden afectar al negocio.

En el Departamento de Sistemas este análisis se realiza de forma reactiva y de acuerdo a la experiencia del Jefe de Sistemas, quien no cuenta con la capacitación adecuada, sin seguir una metodología ni generar la documentación necesaria.

Es por esto que se sugiere a la Gerencia establecer un proceso de análisis, evaluación y gestión de riesgos tecnológicos basados en una metodología y estándares a nivel de Institución que sea del conocimiento de todo el personal.

Asignar un responsable para la gestión de riesgos de de TI que cuente con la experiencia y capacitación adecuadas, así como crear un plan de mitigación de riesgos tecnológicos que se aplique oportunamente.

4.5.8 BAI02 GESTIONAR LA DEFINICIÓN DE REQUISITOS.

La Institución está consciente de la importancia de definir requerimientos de TI para identificar soluciones automatizadas con respecto a hardware, software y servicios de TI que son relevantes para el negocio. Esta actividad es responsabilidad del Jefe del Departamento de Sistemas, que teniendo en cuenta la experiencia adquirida desarrolla un análisis sobre la factibilidad tecnológica y riesgos, posteriormente realiza un análisis costo'beneficio sobre las

necesidades y el resultado final es expuesto en un documento que debe ser aprobado por la Gerencia.

Se propone un enfoque estructurado para identificar las soluciones de TI necesarias para el correcto funcionamiento del negocio, junto a la documentación necesaria que lo respalde. Se recomienda establecer un proceso documentado para determinar las soluciones de TI necesarias y establecer un control de calidad de la documentación generada para las soluciones tecnológicas.

4.5.9 BAI03 GESTIONAR LA IDENTIFICACIÓN Y CONSTRUCCIÓN DE SOLUCIONES

La Cooperativa reconoce la necesidad de tener un proceso definido para adquirir y mantener software aplicativo. En estos momentos realizan procedimientos internos del Departamento de Sistemas para conseguir resultados eficientes de mantenimiento y soporte de las aplicaciones. Para realizar esta actividad no se utiliza una metodología, unicamente se basa en procedimientos establecidos por el jefe de dicho departamento, quien determina las actividades, recursos, tiempo y costos necesarios para su cumplimiento.

Para mejorar esta actividad se propone un proceso definido para adquirir y mantener software aplicativo junto con una metodología estándar que garantice su cumplimiento y genere la documentación necesaria. Además es importante poner especial atención en aspectos tecnológicos como disponibilidad y seguridad para la adquisición de software aplicativo.

4.5.10 BAI05 GESTIONAR LA FACILITACIÓN DEL CAMBIO ORGANIZATIVO.

En la Cooperativa se reconoce la importancia que tiene la producción de documentación para los usuarios, por lo que la documentación que se suministra con los productos adquiridos no es la única que se utiliza en la Institución. Aunque para el desarrollo de la documentación no se utilizan estándares, solamente se cuenta con la experiencia de los responsables de la actividad.

En el Departamento de Sistemas se genera documentación que facilite a los usuarios entender y adaptarse rápidamente a los cambios o actualizaciones que se realicen en los sistemas.

Es por esto que se propone establecer un enfoque uniforme para procedimientos de generación y actualización de manuales de usuarios y de operación, así como involucrar a los usuarios en la mayor parte del proceso de generación de documentos para los propios usuarios, para mejorar la calidad de los mismos debido a la retroalimentación.

4.5.11 DSS04 GESTIONAR LA CONTINUIDAD DEL SERVICIO

La Gerencia de la Cooperativa está consciente de la importancia de identificar los riesgos, vulnerabilidades y amenazas en lo que se refiere a operaciones de TI e infraestructura, pero no cuentan con un plan de continuidad. En estos momentos se encuentran en el desarrollo de un plan de contingencia que pueda minimizar el impacto en caso que se presente algún incidente que atente contra la continuidad de los servicios.

Es por esto que se debe capacitar a los usuarios para que puedan solucionar problemas mínimos sobre los recursos de TI. Establecer un plan de continuidad de los servicios de TI que contemple todas las amenazas posibles. Es importante emitir reportes sobre la disponibilidad de los servicios y clasificar los sistemas y componentes críticos.

4.5.12 DSS05 -GESTIONAR SERVICIOS DE SEGURIDAD.

La Gerencia está consciente de la importancia de la seguridad de los sistemas, es por ello que reconoce la necesidad de desarrollar un plan de Seguridad de Sistemas que contemple los aspectos necesarios para mantener la integridad de la información y proteger los activos de TI. Actualmente solo cuentan con algunas políticas de seguridad que no son suficientes para abarcar todos los aspectos requeridos.

Se recomienda establecer un responsable que garantice la seguridad de los recursos de TI implementando un plan de seguridad en base a un análisis de riesgos, que establezca una documentación para todos los procedimientos de seguridad de TI. Es necesario desarrollar e implementar en la Cooperativa un programa de conciencia sobre seguridad informática y capacitar al personal para que de cumplimiento a las políticas de seguridad establecidas. Además se propone emitir reportes sobre incidentes y problemas relacionados con la seguridad de TI.

4.5.13 MEA01 SUPERVISAR, EVALUAR Y VALORAR EL RENDIMIENTO Y LA CONFORMIDAD

La Gerencia y el Departamento de Sistemas coinciden en la necesidad de que exista en la Cooperativa un proceso de monitoreo y evaluación del desempeño de TI, pero actualmente no está definido, por lo que esta actividad se realiza internamente en el Departamento de Sistemas siguiendo estándares propios. Las métricas de desempeño de TI son proporcionadas por las herramientas propias del Departamento de Sistemas y son evaluadas de acuerdo a la experiencia del jefe de dicho departamento, quien crea un informe con los resultados obtenidos que es entregado a la Gerencia para la evaluación del desempeño y la toma de decisiones.

Se recomienda a la Cooperativa de Ahorro y Créditos Nueva Esperanza, establecer un proceso definido de monitoreo y evaluación del desempeño de TI, junto con reportes que informen acerca de la eficiencia del departamento y que apoyen a las decisiones gerenciales. Deben asignar un responsable que cumpla con el rol de monitoreo y evaluación del desempeño de TI.

4.5.14 MEA02 -SUPERVISAR, EVALUAR Y VALORAR EL SISTEMA DE CONTROL INTERNO.

La Institución es consciente de la necesidad de implementar controles internos a TI, sin embargo no cuentan con un proceso definido para su cumplimiento en el Departamento de Sistemas. Aunque ciertas funciones críticas para el negocio como los cambios que se realizan en bases de datos y aplicaciones, son registradas en un documento que permite mantener el control de los cambios.

Los reportes emitidos por el monitoreo y evaluación del control interno no contemplan suficientes aspectos tecnológicos, por lo que el Jefe de Sistema realiza informes de actividades periódicas que presenta a la Gerencia con el fin de rendir cuentas del cumplimiento de los objetivos de departamento.

Se propone a la Empresa establecer un proceso definido de control interno de TI, que abarque puntos de control e indicadores de su efectividad y eficiencia, con un responsable asignado.

Además se recomienda elaborar un listado de los controles internos críticos para que la Gerencia determine un monitoreo periódico de su efectividad.

4.5.15 MEA03. SUPERVISAR, EVALUAR Y VALORAR LA CONFORMIDAD CON LOS REQUERIMIENTOS EXTERNOS.

La Gerencia se encarga de dar a conocer y hacer cumplir las leyes, regulaciones y contratos con los proveedores. Es por esto que se ha establecido un consejo de vigilancia para controlar los asuntos financieros, mientras que los organismos de control, auditoría interna y externa, se encargan de asegurar el cumplimiento tanto en el aspecto financiero como tecnológico. La evaluación del cumplimiento de los requerimientos regulatorios se realiza periódicamente con el fin de detectar las anomalías, de manera que se puedan corregir de forma oportuna.

Se recomienda a la Institución realizar un monitoreo interno constante acerca de las nuevas regulaciones de requerimientos financieros y legislación de privacidad, con el fin de asegurar su cumplimiento, así como la necesidad de crear un programa de conciencia y entrenamiento sobre requisitos legales y regulatorios que afectan a la Cooperativa.

Sería eficiente implementar políticas y procedimientos para garantizar el cumplimiento de los reglamentos y obligaciones contractuales, además de desarrollar contratos pro-forma y procesos legales estándar para minimizar los riesgos asociados con las obligaciones contractuales.

4.6 COMPROBACIÓN DE LA HIPÓTESIS

4.6.1 HIPÓTESIS

El uso de una guía de implementación de las tecnologías de la información, aplicando el modelo COBIT, para auditorías en entidades financieras permite la disminución de errores en su proceso de aplicación.

4.6.2 ANÁLISIS DE INDICADORES

El resultado final del análisis de los datos obtenidos después de haber aplicado COBIT 5 a los procesos tecnológicos de la Cooperativa, se representa en la Tabla 5.

Para ello se midieron los indicadores en una escala del 1 al 10, tomando como valor total para obtener el por ciento de efectividad, 40, ya que se están analizando 4 indicadores.

Indicadores	Aplicando COBIT		
	Siempre	A veces	Nunca
Seguridad de la información (10)	9.2	7.5	2.5
Disponibilidad de la información (10)	8.5	7.0	2.0
Actividades para la gestión interna de las TICs (10)	9.0	6.7	2.3
Actividades de Aseguramiento (10)	9.0	7.5	3.0
Total (40)	37.5	28.7	9.8
Porcentaje	93.75 %	71.75 %	24.50%

Tabla 20 Análisis de indicadores.

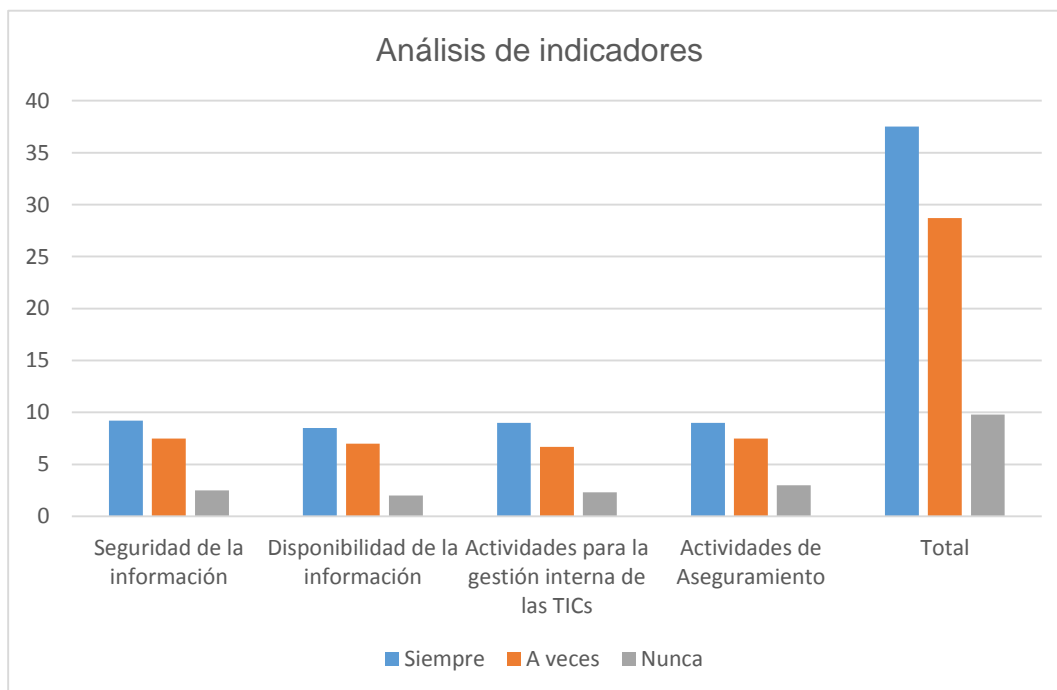


Figura 11 Análisis de indicadores.

4.6.3 COMPROBACIÓN DE LA HIPÓTESIS

4.6.3.1 COMPROBACIÓN

A continuación se muestra el gráfico que representa de los porcentajes totales de la Gestión de las Tecnologías de la Información con la Aplicación de COBIT 5 en la Cooperativa de Ahorro y Crédito Nueva Esperanza que nos permite la comprobación de la hipótesis planteada en el presente trabajo.

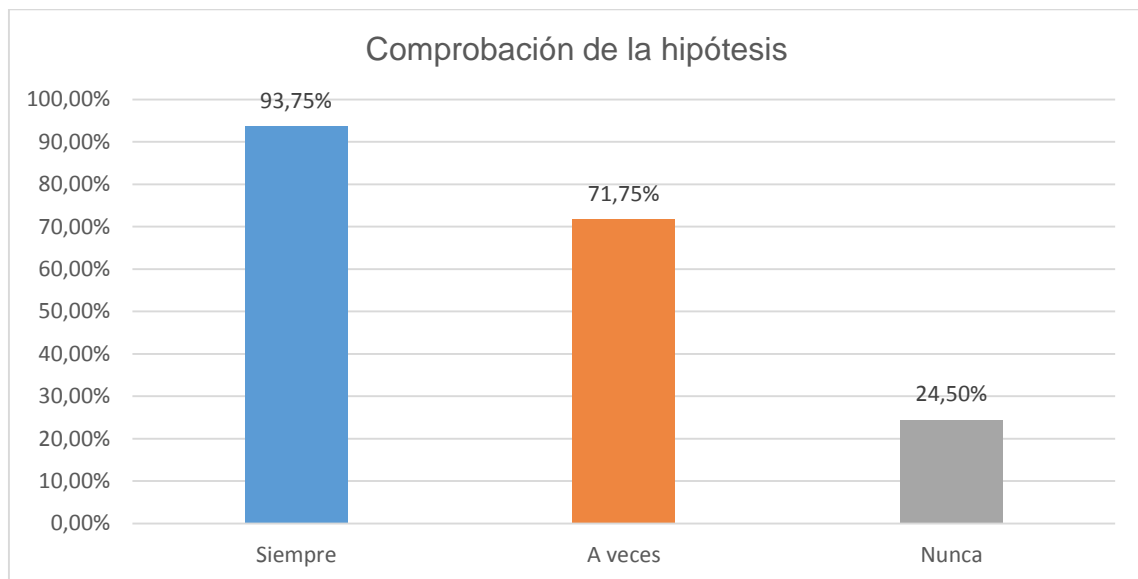


Figura 12 Comprobación de la hipótesis aplicando COBIT 5.

4.6.3.2 DECISIÓN

Como se observa en la Figura 12 la guía planteada para el uso de la guía aplicando la metodología COBIT 5 obtiene el **93.75 %** de efectividad, cuando se aplica en ocasiones, es decir no siempre, se obtiene un 71.75 % y cuando no se aplica se obtiene un 24.50 %. Por lo que podemos decidir que la guía propuesta en el presente trabajo nos permite obtener resultados más eficientes y seguros en el momento de realizar la auditoría informática en la Cooperativa de Ahorro y Créditos Nueva Esperanza. De esta forma se acepta la hipótesis planteada.

CAPÍTULO V CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

Los procesos analizados en el presente trabajo fueron seleccionados teniendo en cuenta las necesidades actuales de la Cooperativa de Ahorro y Crédito Nueva Esperanza y a la importancia que tienen para el cumplimiento de los objetivos de negocio. El resultado de la evaluación de la gestión de las TICs en la Empresa será de gran utilidad para que la Gerencia pueda conocer el estado actual de gestión que se lleva a cabo por el Departamento de Sistemas, y pueda tomar acciones en base a las recomendaciones.

A través del uso del marco de trabajo COBIT 5 se ha logrado identificar cuáles son los aspectos que deben tener en cuenta para mejorar los procesos en el Departamento de Sistemas.

Las directrices de auditoría de COBIT 5 se tomaron como una guía para la planificación de la evaluación realizada ya que ofrecen alternativas para determinar las posibles actividades que se realizan dentro de la evaluación de TI.

Como resultado de este trabajo podemos decir que la falta de personal del Departamento de Sistemas genera sobrecarga de trabajo entre el personal de Sistemas, lo que hace que se cumplan tareas de acuerdo a la disponibilidad de tiempo del personal aunque no estén asignadas a su cargo las actividades dentro del Manual de Perfiles. Además, se tiene dependencia de la experiencia y conocimiento del personal de Sistemas para realizar actividades que no constan en el Manual de Perfiles y que son relevantes para dar soporte en la toma de decisiones.

El análisis de riesgo que se realiza en la Empresa se centra mayormente en aspectos financieros descuidando la parte tecnológica, por lo que no existe garantía de la mitigación de los riesgos ni de su impacto en el negocio.

A pesar que la Gerencia reconoce la importancia de Gestión de TICs no ha tomado medidas para garantizar una adecuada gestión de los recursos, lo que supone una cierta deficiencia en aspectos importantes del Departamento de Sistemas.

5.2 RECOMENDACIONES

Una vez realizada la auditoría informática se recomienda lo siguiente:

Aplicar el plan de acción planteado como resultado de este proyecto.

Alinear los objetivos estratégicos con las políticas que se tiene planteadas en la cooperativa, y a su vez monitorear el cumplimiento de los mismos.

Realizar el levantamiento de procesos del Departamento de Sistemas para establecer una gestión de TICs en base a estándares y buenas prácticas de la industria que garanticen la seguridad e integridad de los servicios de TI.

Identificar los recursos de Ti críticos para el negocio con el fin de administrarlos adecuadamente para poder satisfacer los requerimientos del negocio.

Concientizar al personal y a la alta dirección de la cooperativa sobre la importancia y el valor que posee la tecnología de información.

Teniendo en cuenta la experiencia adquirida en el presente proyecto, se considera importante que el personal tanto del área de sistemas como de auditoría interna, y la alta dirección reciban una inducción en la metodología de auditoría informática, para que su aplicación sea más productiva y los resultados de la evaluación sean elementos de juicio para toma de decisiones.

En la planificación de la auditoría informática es necesario identificar correctamente los elementos que intervienen, de modo que se tenga una visión global y concreta de los objetivos de evaluación del proceso de auditoría.

Un elemento muy importante en el éxito de una auditoría es el tiempo asignado para la planificación de la misma, pues en esta fase se identifican las directrices de su realización, por ello se recomienda tomar en cuenta variables como el tamaño de la organización, la cantidad de procesos a evaluar, la metodología a utilizar, conformación del equipo auditor, entre otros, para que el resultado de la planificación sea la hoja de trabajo principal del auditor.

GLOSARIO DE TÉRMINOS

Auditor: Persona que efectúa una auditoría

Auditoría: Examen de las operaciones de una empresa efectuado por especialistas ajenos a ella y con objetivos de evaluar la situación de la misma.

Auditoría basada en riesgos: Es el examen de las operaciones de una empresa que le permite al auditor obtener una seguridad razonable de que en los estados financieros no existan declaraciones erróneas causadas por fraude o error.

COBIT: Acrónimo de “Control Objectives for Information and related Technology” (Objetivos de Control para la Información y Tecnologías Relacionadas), fue desarrollado en específico para el ámbito de las TIC.

COSO: Modelo de control interno.

ITIL: Acrónimo de “Information Technology Infrastructure Library” (Biblioteca sobre infraestructura de la información tecnológica), norma de mejores prácticas para la administración de servicios de Tecnología de Información.

TICS: Tecnologías de la información y las Comunicaciones.

Protocolos: Conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red.

TI: Tecnología de Información, conjunto de técnicas que permiten la captura, almacenamiento, transformación, transmisión y presentación de la información generada o recibida a partir de procesos, de manera que pueda ser organizada y utilizada en forma consistente y comprensible por los usuarios que estén relacionados con ella. Incluye elementos de hardware, software, telecomunicaciones y conectividad. (It Governance Institute. *Cobit 4.1*. (2007)).

AI: Auditoría Informática.

Stakeholders: Se refiere a las **partes interesadas**.

- Externas: sociedad en general, clientes, proveedores, autoridad de contralor, auditores externos.
- Internas: órgano de administración y de gobierno, responsables de los procesos de negocios, responsables del sistema de registro contable, responsables de la TI, responsables del cumplimiento, auditores internos.

BIBLIOGRAFÍA

Abu-Masa, A. (2008). Exploring the importance and Implementation of COBIT Processes in Saudi Organizations. Extraído el 18 Julio, 2015 de Emerald Insight. www.emeraldinsight.com/0968-5227.htm.

Aguilera, A., & Riascos, S. (2009). Direccionamiento Estratégico Apoyado en las TIC. Estudios Gerenciales, 25 (111). p 127-143.

Alcántara, P. (2009). El auditor frente a la evolución tecnológica. Argentina: El Cid Editor. Apuntes. p 4. <http://site.ebrary.com/lib/uasuaysp/Doc?id=10316808&ppg=4>

Apuntes de Auditoría Informática. (2009). México, <http://mx.oocities.com/acadentorno/aui3.pdf>

Armenta Fonseca, L. 12 de marzo de 2014. Cómo determinar la Capacidad de los Procesos en COBIT 5 http://es.slideshare.net/lorenzo_kila/cmo-determinar-la-capacidad-de-los-procesos-de-cobit-5

Brito, JA; Echevarría, PB. (2009). Creación de un marco de control para la administración del riesgo operativo relacionado con la tecnologías de la información como modelo para las cooperativas de ahorro y crédito del Ecuador. Extraído el 17 Julio, 2015 de <http://www.dspace.espol.edu.ec/xmlui/handle/123456789/6176>

Castilla Plaza, C. (2006) Implicaciones de las tecnologías de la información en la gestión del sistema empresa. España: Universidad Complutense de Madrid. p 14.

Castellanos, W. (2007). Gestión de TI para el negocio. p. 11-23.

Caushin, R. (2013). El Proceso de la Auditoría de Sistemas de Información. I-SEC Information Security Inc. p 45-51. Extraído el 24 Agosto, 2015 de <http://site.ebrary.com/lib/uasuaysp/Doc?id=10272178&ppg=133>.

COBIT 4.1, 2007 <http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf>

COBIT Focus Volumen 1, enero de 2014 <http://www.isaca.org/Knowledge-Center/cobit/cobit-focus/Pages/COBIT-Focus-Volumen-1-enero-de-2014.aspx>

COBIT 5 aplicado al sistema de registro contable informático argentino <http://www.isaca.org/COBIT/focus/Pages/COBIT-5-Applied-to-the-Argentine-Digital-Accounting-System-Spanish.aspx>

COBIT 5 (2012). Implementación, ISACA, Estados Unidos.

Council, C. (2006). Implementing COBIT in Higher Education: Practices That Work Best. Extraído el 14 Agosto, 2015 de ISACA <http://www.isaca.org/Journal/archives/2006/Volume-5/Pages/JOnline-Implementing-COBIT-in-Higher-Education-Practices-That-Work-Best1.aspx>

Dionicio Teo, L.G. Evaluación de controles según el modelo COBIT, para la adquisición y mantenimiento de aplicaciones informáticas en el departamento de informática de una empresa distribuidora de vehículos automotores. Tesis, Facultad de Ciencias Económicas. Universidad de San Carlos de Guatemala. Mayo 2011. Pág. 44

Durán Jacobo, M.A. 13 de septiembre de 2010. Diferentes modelos de control aplicados a la auditoría informática <http://es.scribd.com/doc/38284391/MODELOS-DE-CONTROL-DE-AUDITORIA-INFORMATICA#scribd>

Echenique J. y McGraw H. (2001). Auditoría en Informática.

Freire, JR. (2011). La auditoría informática y su incidencia en la disponibilidad de los sistemas de información en la cooperativa de ahorro y crédito El Sagrario Ltda. Extraído el 12 Julio, 2015 de <http://repositorio.uta.edu.ec/jspui/handle/123456789/1882>

Graciela Braga, COBIT Focus, 5 Enero 2015.

ISACA. <http://www.isaca.org/About-ISACA/Licensing-and-Promotion/Pages/COBIT-Usage-Guidelines.aspx>

ISACA. (2010). COBIT Case Study: Implementing COBIT for IT Governance, Risk and Compliance at Ecopetrol S.A. Extraído el 12 Febrero, 2015 de ISACA: <http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-StudyEcopetrol.aspx>.

ISACA. (2011). Cobit 5 the Framework (Exposure draft). IL, USA: CRISC.

ISACA, 2011, COBIT 5 - Cambios de la nueva versión <http://www.isaca.org/Groups/Professional-English/cobit-5-use-it-effectively/Pages/ViewDiscussion.aspx?PostID=18>

IT Governance Institute, COBIT 3rd Edition Management Guidelines, Rolling Meadows, IL, USA, 2000.

It Governance Institute. Cobit 4.1. (2007), Estados Unidos, [En Línea]. Disponible en <http://www.isaca.org/Knowledge-Center/cobit/Documents/cobit4.1spanish.pdf>

López, F. & Soriano, N. (2012). La gestión de la tesorería. Barcelona: Libros de cabecera. p 92-102.

Maggio, M. (2012). Enriquecer la enseñanza. Cap. 4. Los nuevos entornos y su enseñanza. Buenos Aires: Editorial PAIDOS.

Malbernat, L. (2010). Tecnologías educativas e innovación en la Universidad. Extraído el 21 Julio, 2015 de: LaCapitalmdp.com

Manual de contingencia Sistema Financiero de la Cooperativa de Ahorro y Créditos Nueva Esperanza.

Manual de Perfiles Ocupacionales por Competencias para la Cooperativa de Ahorro y Créditos Nueva Esperanza. (2012).

MANUAL PROCEDIMIENTOS COOPERATIVA NUEVA ESPERANZA. (2015).

Naranjo, MJ. (2010). Auditoría administrativa a la Jefatura de Recursos Humanos de la Empresa Eléctrica Riobamba S.A. Extraído el 21 Julio, 2015 de <http://dspace.espoch.edu.ec/handle/123456789/1800>

Orta Pedroza, O.J. 4 de septiembre de 2014. Análisis de madurez y capacidad de procesos según COBIT 5. <http://gesegtic.blogspot.com/2014/09/analisis-de-madurez-y-capacidad-de.html>

Piattini M. y Del Peso E. (2007). Auditoría Informática, un enfoque práctico. México

Quintanilla, M. (2015) Libro Guía Texto para Silabo “Auditoría de Sistemas Informáticos II” <http://www.mqr.gqnu.net/fca/SILABO2.pdf>

Simón, C.S. (2006). Auditoría Informática. España. <http://www.scaridad.com/files/Apuntes%20de%20AI.pdf>

Steven Babb, 2014 Are COSO 2013 and COBIT 5 Compatible?

<http://www.isaca.org/COBIT/focus/Pages/Are-COSO-2013-and-COBIT-5-Compatible.aspx>

ANEXOS

1. Cronograma de implementación.

Nombre de tarea	Duración
Estudio preliminar	40 días
Solicitud de información	10 días
Recopilación de información	10 días
Ordenamiento de la información	20 días
Planeación de la auditoría	60 días
Comprensión del control interno	5 días
Desarrollo de la estrategia de auditoría	10 días
Identificación de procesos de la Cooperativa a evaluar	10 días
Determinar procesos de COBIT 5	15 días
Asociar procesos de la cooperativo con los procesos de COBIT 5	18 días
Realizar cronograma	2 días
Ejecución de la auditoría	70 días
Conformación del grupo a evaluar	5 días
Recolección y síntesis de la evaluación	30 días
Determinación del nivel de madurez de los procesos	10 días
Análisis de los resultados	25 días
Informe final	20 días
Revisión de los papeles de trabajo.	3 días
Elaboración del Informe	15 días
Elaboración de la carta de presentación	2 días
Total	190 días

2. Comprobante directivas 12/02/2016



Fecha de Generación de Documento: 12/febrero/2016

Validez de Documento: 30 días a partir de la fecha de generación

COMPROBANTES DE DIRECTIVOS DE ORGANIZACIONES DE LA ECONOMÍA POPULAR Y SOLIDARIA

DATOS DE LA ORGANIZACIÓN

SECTOR: COOP-SFPS
RUC: 0691720721001
RAZÓN SOCIAL: COOPERATIVA DE AHORRO Y CREDITO NUEVA ESPERANZA LTDA. - RIOBAMBA
PROVINCIA: CHIMBORAZO
CANTÓN: RIOBAMBA
PARROQUIA: VELASCO
DIRECCIÓN: VENEZUELA Y FRANCIA ESQUINA 28-60 FRANCIA
TELÉFONO: 032942542
SEGMENTO NIVEL: SEGMENTO 4
ESTADO: ACTIVA

DIRECTIVOS

REPRESENTANTE LEGAL (GERENTE): CANTUÑA ADRIANO
OSWALDO DEMETRIO
PRESIDENTE: FERNANDEZ CANDO
MARGARITA ISABEL
SECRETARIO: JARA ULLE ROSARIO
ELIZABETH
PRESIDENTE CONSEJO DE VIGILANCIA: NAUÑAY GUAMAN BLANCA
ISABEL

La información constante en el presente documento, corresponde a la recibida de la organización, quien asume cualquier tipo de responsabilidad por error o falsedad en la misma. En caso de querer validar ésta información deberá ingresar en la página web: www.seps.gob.ec

SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

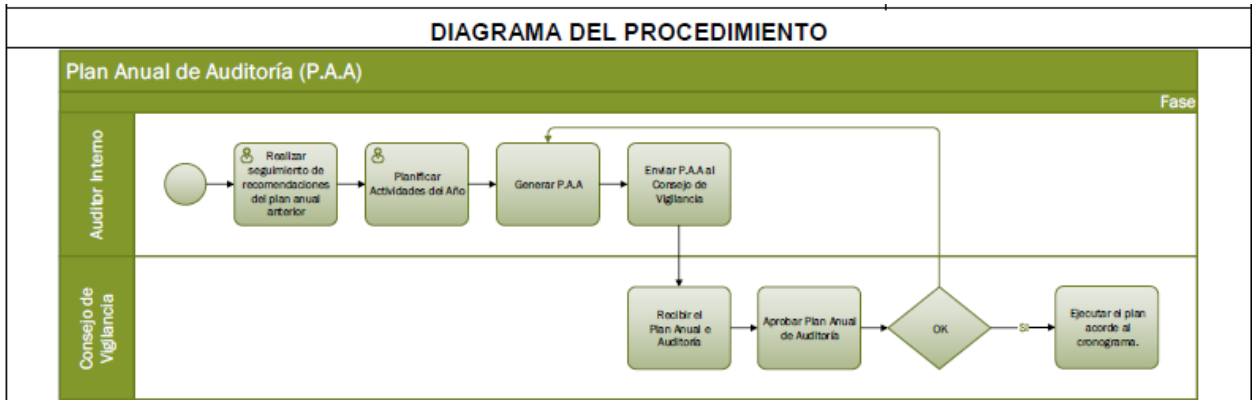


3. Comprobante Existencia Legal 12-02-2016

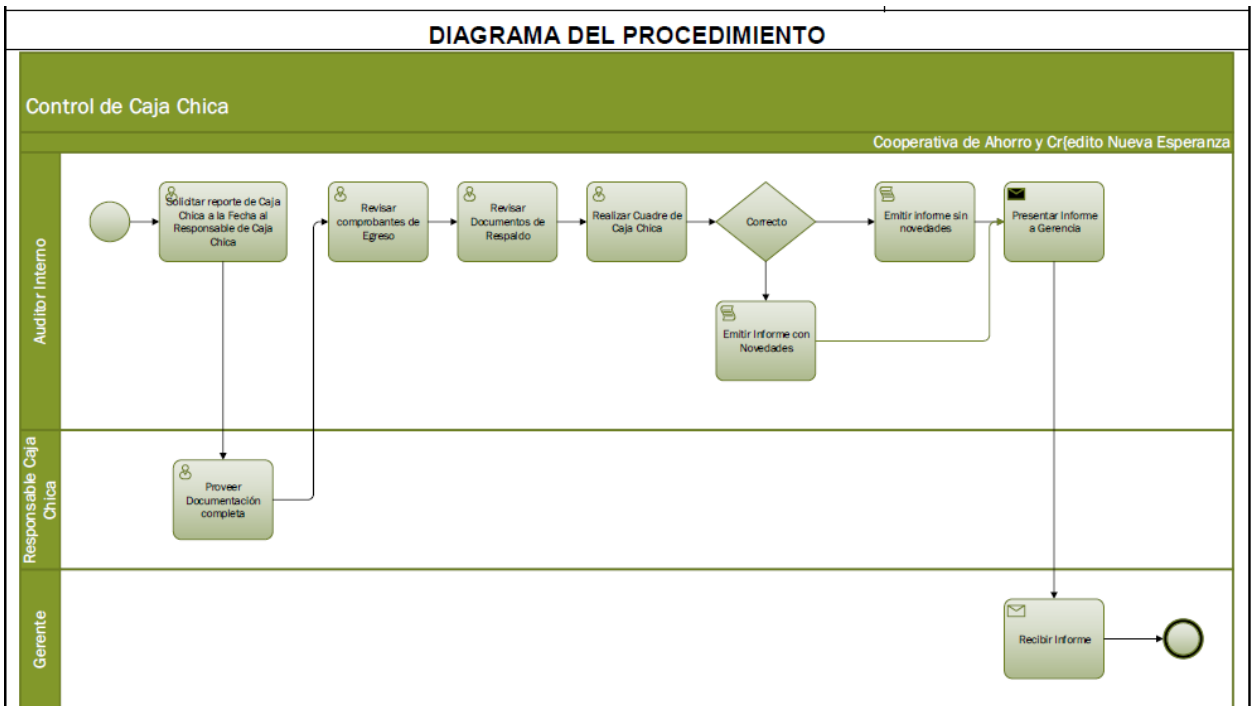
	
Fecha de Generación de Documento: 12/febrero/2016	
Validez de Documento: 30 días a partir de la fecha de generación	
COMPROBANTE DE EXISTENCIA LEGAL DE ORGANIZACIONES DE LA ECONOMÍA POPULAR Y SOLIDARIA	
Revisado el Catastro Digital de Organizaciones de esta Superintendencia, consta la siguiente información de la COOPERATIVA DE AHORRO Y CREDITO NUEVA ESPERANZA LTDA. - RIOBAMBA	
DATOS DE LA ORGANIZACIÓN	
No. RESOLUCIÓN CONSTITUCIÓN/ADECUACIÓN: SEPS-ROEPS-2013-001556	
FECHA DE RESOLUCIÓN CONSTITUCIÓN/ADECUACIÓN: 05/31/2013	
RUC:	0691720721001
SECTOR:	COOP-SFPS
RAZÓN SOCIAL:	COOPERATIVA DE AHORRO Y CREDITO NUEVA ESPERANZA LTDA. - RIOBAMBA
PROVINCIA:	CHIMBORAZO
CANTÓN:	RIOBAMBA
PARROQUIA:	VELASCO
SEGMENTO / NIVEL:	SEGMENTO 4
ESTADO:	ACTIVA
La información constante en el presente documento, corresponde a la recibida de la organización, quien asume cualquier tipo de responsabilidad por error o falsedad de la misma. En caso de querer validar esta información deberá ingresar en la página web: www.seps.gob.ec	
El presente comprobante carecerá de validez probatoria en un proceso judicial; para el efecto, se solicitará la respectiva certificación.	
SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA	
	

4. Principales procesos que intervienen en la auditoría de la Cooperativa. Manual Procedimientos (2015).

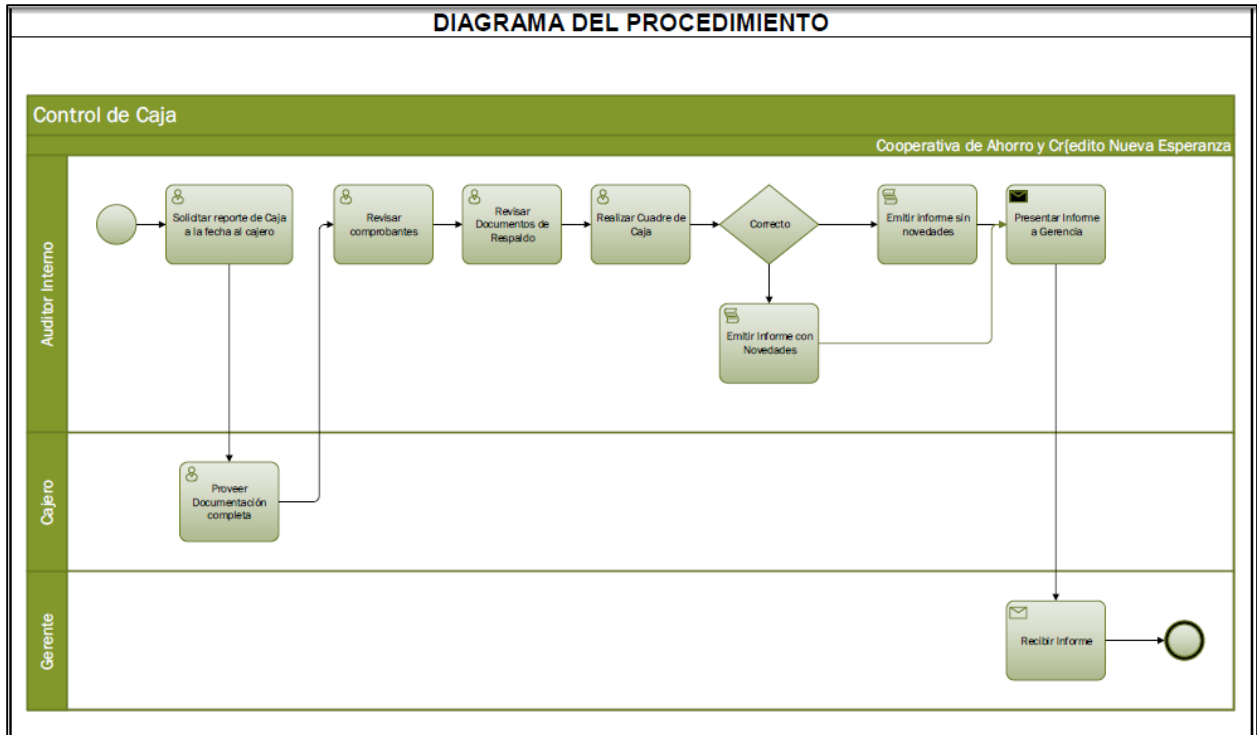
4.1 Plan anual de auditoría



4.2 Control de Caja Chica



4.3 Control de Caja



4.4 Control de File de Crédito

