

ESCUELA POLITÉCNICA DEL EJÉRCITO

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

DPTO. DE CIENCIAS DE LA COMPUTACIÓN

**“AUDITORÍA INFORMÁTICA DE LA COOPERATIVA DE
AHORRO Y CRÉDITO “ALIANZA DEL VALLE” LTDA.
APLICANDO COBIT 4.0”**

Previa a la obtención del Título de:

INGENIERO EN SISTEMAS E INFORMÁTICA

REALIZADO POR:

GABRIELA FERNANDA BARROS MARCILLO

ANDREA ERIKA CADENA MARTEN

SANGOLQUÍ, 10 de Enero del 2012

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por las Srtas. GABRIELA FERNANDA BARROS MARCILLO y ANDREA ERIKA CADENA MARTEN como requerimiento parcial a la obtención del título de INGENIERAS EN SISTEMAS E INFORMÁTICA.

Sangolquí, 10 de Enero del 2012

ING. MARIO RON

DEDICATORIA

A mis Padres, quienes durante toda mi vida me han brindado la fuerza, confianza, ánimo y apoyo necesario; siendo mi apoyo incondicional en toda esta etapa de mi vida, también es dedicada a mi hermano que es el motivo de mi lucha diaria y, por el que me esfuerzo día a día.

Rolando Neidy y Héctor

ANDREA CADENA

DEDICATORIA

Dedico este proyecto de tesis a DIOS, a mi familia y mi novio. A Dios porque ha estado conmigo a cada paso que doy, cuidándome y dándome fortaleza para continuar, a mi familia, quienes a lo largo de mi vida han velado por mi bienestar y educación siendo mi apoyo en todo momento. Depositando su entera confianza en cada reto que se me presentaba sin dudar ni un solo momento en mi inteligencia y capacidad. A mi novio, compañero inseparable apoyo en los momentos difíciles y aliento para seguir adelante y no desmayar. Es por ellos que soy lo que soy ahora. Los amo con mi vida.

GABRIELA BARROS

AGRADECIMIENTO

A mis padres por ser mi ejemplo a seguir, por brindarme todo el amor y apoyo durante mi vida, a mi hermano por darme la fuerza para seguir adelante a pesar de todo, a mi enamorado por ser mi soporte, a mi familia por siempre estar a mi lado, a la Escuela Politécnica del Ejército por todas las enseñanzas recibidas, a los ingenieros que ayudaron en la elaboración de este proyecto: Ing. Mario Ron, Eco. Gabriel Chiriboga; por su guía en todas las fases de la tesis y a todas las personas que de una u otra forma ayudaron a la culminación de esta meta.

ANDREA CADENA

AGRADECIMIENTO

En primer lugar a DIOS por haberme guiado por el camino de la felicidad hasta ahora; en segundo lugar a cada uno de los que son parte de mi familia a mi PADRE Víctor Barros, mi MADRE Rosario Marcillo, mis hermanos y sobrinos por siempre haberme dado su fuerza y apoyo incondicional que me han ayudado y llevado hasta donde estoy ahora. A mi compañera de tesis y amiga Andrea Cadena, a la Escuela Politécnica del Ejército por todas las enseñanzas recibidas y, de una manera muy especial agradezco a quienes fueron guía y apoyo para culminar este proyecto Ing. Mario Ron y Eco. Gabriel Chiriboga.

GABRIELA BARROS

TABLA DE CONTENIDOS

| | |
|--|-----|
| ANEXOS | 116 |
| Anexo A | |
| Hojas de Evaluación | 116 |
| Anexo B | |
| Carpeta de Evidencias | 149 |
| Anexo C | |
| Lista de Documentación Solicitada | 213 |
| Anexo D | |
| INFORME EJECUTIVO..... | 215 |
| Anexo E | |
| INFORME DETALLADO | 221 |
| Anexo F | |
| NIVEL DE MADUREZ DE LA COOPERATIVA | 250 |
| Anexo G | |
| PROPUESTA DE SERVICIOS DE AUDITORÍA EN INFORMÁTICA..... | 256 |
| BIBLIOGRAFÍA | 261 |
| CAPÍTULO I | 18 |
| 1.1 GENERALIDADES | 18 |
| 1.2. EL PROCESO DE LA AUDITORÍA INFORMÁTICA..... | 27 |
| 1.3. CLASIFICACIÓN DE LOS CONTROLES TI..... | 34 |
| CAPÍTULO II | 37 |
| 2.1. INTRODUCCIÓN..... | 37 |
| 2.2. CONTENIDO (PRODUCTOS COBIT) | 38 |
| 2.3. GENERALIDADES DEL MODELO COBIT | 42 |
| CAPÍTULO III | 54 |
| 3.1. SITUACIÓN ACTUAL DE LA ENTIDAD | 54 |
| 3.2. APLICACIÓN DEL MODELO COBIT A LA COOPERATIVA DE AHORRO Y CREDITO “ALIANZA DEL VALLE” | 81 |
| 3.3. INVESTIGACIÓN DE CAMPO..... | 87 |
| CAPÍTULO IV..... | 107 |
| 4.1. INTRODUCCIÓN..... | 107 |
| 4.2. RESUMEN EJECUTIVO..... | 107 |
| 4.3. DESCRIPCIÓN DEL TRABAJO EFECTUADO | 109 |

| | |
|--|-----|
| 4.4. RESULTADOS – INFORME DE LAS RECOMENDACIONES | |
| ACORDADAS CON LAS AUTORIDADES PERTINENTES | 110 |
| CAPÍTULO V | 114 |
| ÍNDICE DE GRÁFICAS | 8 |
| ÍNDICE DE TABLAS | 7 |
| PRÓLOGO | 17 |
| RESUMEN | 16 |

ÍNDICE DE TABLAS

| | |
|--|----|
| TABLA 2: MATRIZ COBIT VS ITIL, COSO | 50 |
| TABLA 3: MATRIZ DE RIESGOS..... | 87 |
| TABLA 4:MATRIZ DE INVESTIGACIÓN DE CAMPO | 97 |

ÍNDICE DE GRÁFICAS

| | |
|---|----|
| GRÁFICA 1:PIRÁMIDE DE PROCESOS..... | 27 |
| GRÁFICA 2:PAQUETE DE PROGRAMAS DE COBIT | 39 |
| GRÁFICA 3: PRINCIPIOS BÁSICOS DE COBIT | 43 |
| GRÁFICA 4:CUBO COBIT | 45 |
| GRÁFICA 5:NIVELES DE ACTIVIDADES DE TI | 46 |
| GRÁFICA 6:MARCO DE COBIT | 49 |
| GRÁFICA 7:ESTRUCTURA ORGANIZACIONAL..... | 59 |
| GRÁFICA 8: AREA OCUPACIONAL | 60 |
| GRÁFICA 9:GRUPO OCUPACIONAL | 60 |
| GRÁFICA 10:OCUPACIONES | 61 |
| GRÁFICA 11:ESTRUCTURA ORGANIZACIONAL DEL AREA DE SISTEMAS | 68 |
| GRÁFICA 12: ESPECIFICACIÓN DE SERVIDORES..... | 79 |
| GRÁFICA 13:ESQUEMA DE LA RED LAN/ WAN | 80 |

GLOSARIO DE TÉRMINOS

Alcance de la auditoría.- El marco o límite de la auditoría y las materias, temas, segmentos o actividades que son objeto de la misma.

Alta gerencia.-La alta gerencia está compuesta por una cantidad de personas comparativamente pequeña y es la responsable de administrar toda la organización. Estas personas reciben el nombre de ejecutivos. Establecen las políticas de las operaciones y dirigen la interacción de la organización con su entorno.

Amenaza.- Cualquier aspecto o escenario que pueda ocasionar que un riesgo se convierta en incidente, o sea, que llegue a realizarse.

Archivos de sistema.- Son aquellos archivos de uso exclusivo del sistema operativo. Estos archivos no pueden ser eliminados normalmente por el usuario o el sistema le advierte que se dispone a eliminar un fichero necesario para su correcto funcionamiento.

Auditor.- Persona que efectúa una auditoría.

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

Auditoría de sistema. Es la revisión que se dirige a evaluar los métodos y procedimientos de uso en una entidad, con el propósito de determinar si su diseño y aplicación son correctos; y comprobar el sistema de procesamiento de información como parte de la evaluación de control interno; así como para identificar aspectos susceptibles de mejorarse o eliminarse.

Auditoría de tecnologías de la información. Consiste en el examen de las políticas, procedimientos y utilización de los recursos informáticos; confiabilidad y validez de la información, efectividad de los controles en las áreas, las

aplicaciones, los sistemas de redes y otros vinculados a la actividad informática.

Bases de Datos.- Colección de datos pertenecientes a un mismo contexto, organizada de tal modo que el ordenador pueda acceder rápidamente a ella. Una base de datos relacionar, es aquella en la que las conexiones entre los distintos elementos que forman la base de datos, están almacenadas explícitamente con el fin de ayudar a la manipulación y el acceso a éstos.

Bitácoras.- Es como el "diario" de algunos programas donde se graban todas las operaciones que realizan, para posteriormente abrirlas y ver qué es lo que ha sucedido en cada momento.

Capacitación.- Toda acción organizada y evaluable que se desarrolla en una empresa para: modificar, mejorar y ampliar los conocimientos; habilidades y actitudes del personal, generando un cambio positivo en el desempeño de sus tareas.

COBIT: Control Objectives for Information and related Technology (Objetivos de Control para Tecnología de la Información y Relacionadas).

Cliente.- Cliente o "programa cliente", es aquel programa que permite conectarse a un determinado sistema, servicio o red.

Cliente-Servidor.- Se denomina así, al binomio consistente en un programa cliente que consigue datos de otro llamado servidor, sin tener que estar obligatoriamente ubicados en el mismo ordenador. Esta técnica de consulta 'remota' se utiliza frecuentemente en redes como 'Internet'.

Eficacia.- Capacidad de lograr el efecto que se desea o se espera.

Eficiencia.- Conjunto de atributos, que se refieren a las relaciones entre el nivel de rendimiento del software y, la cantidad de recursos utilizados bajo unas condiciones predefinidas.

Estándar.- Es toda regla aprobada o práctica requerida, para el control de la performance técnica y de los métodos utilizados por el personal involucrado en el Planeamiento y Análisis de los Sistemas de Información.

Evaluación.- Es el proceso de recolección y análisis de información y, a partir de ella, presentar las recomendaciones que facilitarán la toma de decisiones.

Elemento del modelo.- Es una abstracción destacada del sistema que está siendo modelado.

Evaluación de Riesgo.- Es el proceso utilizado para identificar y evaluar riesgos y su impacto potencial.

Evidencia.- Es toda información que utiliza el AI, para determinar, si el ente o los datos auditados siguen los criterios u objetivos de la auditoría.

Evidencia de auditoría. Son las pruebas que obtiene el auditor, durante la ejecución de la auditoría, que hace patente y manifiesta la certeza o convicción, sobre los hechos o hallazgos, que prueban y demuestran claramente éstos, con el objetivo de fundamentar y respaldar sus opiniones y conclusiones.

Estándares: Es una especificación o modelos que regulan la realización de ciertos procesos o la fabricación de componentes para garantizar la interoperabilidad.

Hallazgos. Son evidencias, como resultado de un proceso de recopilación y síntesis de información: la suma y la organización lógica de información, relacionada con la entidad, actividad, situación o asunto que se haya revisado o evaluado, para llegar a conclusiones al respecto o para cumplir alguno de los objetivos de la auditoría. Sirven de fundamento a las conclusiones del auditor y, a las recomendaciones que este formula para que se adopten las medidas correctivas.

Herramienta.- Es el conjunto de elementos físicos utilizados para llevar a cabo las acciones y pasos definidos en la técnica.

Herramienta de Control.- Son elementos de software, que permiten definir uno o varios procedimientos de control, para cumplir una normativa y un objetivo de control.

Herramientas de Software de Auditoría.- Son programas computarizados, que pueden utilizarse para brindar información para uso de auditoría.

Informática.- Ciencia que estudia el tratamiento automático de la información en computadoras, dispositivos electrónicos y, sistemas informáticos.

Informe de Auditoría.- Es el producto final del Auditor de SI; constituye un medio formal de comunicar los objetivos de la auditoría, el cuerpo de las normas de auditoría que se utilizan, el alcance de auditoría y, los hallazgos, conclusiones y recomendaciones.

Integridad.- Consiste en que solo los usuarios autorizados puedan variar los datos.

Irregularidades.- Son las violaciones intencionales a una política gerencial establecida, declaraciones falsas deliberadas u omisión de información del área auditada o de la organización.

Infraestructura tecnológica.- Conjunto de elementos de hardware (servidores, puestos de trabajo, redes, enlaces de telecomunicaciones, etc.), software (sistemas operativos, bases de datos, lenguajes de programación, herramientas de administración, etc.) y servicios (soporte técnico, seguros, comunicaciones, etc.); que en conjunto dan soporte a las aplicaciones (sistemas informáticos) de una empresa.

Jerarquía.- Es la disposición de personas, animales o cosas, en orden ascendente o descendente, según criterios de clase, poder, oficio, categoría, autoridad o cualquier otro asunto que conduzca a un sistema de clasificación.

Metodología: Se refiere a los métodos de investigación que se siguen para alcanzar una gama de objetivos en una ciencia. Aún cuando el término puede ser aplicado a las artes, cuando es necesario efectuar una observación o análisis más riguroso o explicar una forma de interpretar la obra de arte. En resumen, son el conjunto de métodos que se rigen en una investigación científica o en una exposición doctrinal.

Norma.- Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción, así como el correcto desarrollo de una actividad.

Normas de auditoría: Constituyen el conjunto de reglas que deben cumplirse, para realizar una auditoría con la calidad y eficiencia indispensables.

Objetivo de la auditoría. Propósito o fin que persigue la auditoría, o la pregunta que se desea contestar por medio de aquella. Auditoría.

Objetivo de Control.- Son declaraciones sobre el resultado final deseado o propósito a ser alcanzado, mediante las protecciones y los procedimientos de control. Son los objetivos a cumplir en el control de procesos.

Ofimática.- Es el sistema informatizado que genera, procesa, almacena, recupera, comunica y presenta datos relacionados con el funcionamiento de la oficina.

Outsourcing.- Es un contrato a largo plazo de un sistema de información o proceso de negocios, a un proveedor de servicios externos.

Políticas.- Conjunto de disposiciones documentadas que regulan el comportamiento de un grupo de individuos.

Política interna.- Conjunto de normas, reglas y disposiciones que regulan el comportamiento, las responsabilidades y las restricciones del personal de una empresa.

Prevención.- Adopción de medidas encaminadas a impedir que se produzcan deficiencias físicas, mentales y sensoriales (prevención primaria) o a impedir que las deficiencias, cuando se han producido, tengan consecuencias físicas, psicológicas y sociales negativas.

Procedimientos de Control.- Son los procedimientos operativos de las distintas áreas de la empresa, obtenidos con una metodología apropiada, para la consecución de uno o varios objetivos de control y, por tanto deben estar documentados y aprobados por la Dirección.

Procedimientos Generales de Auditoría.- Son los pasos básicos en la realización de una auditoría.

Pruebas de Cumplimiento.- Son aquellas evidencias que determinan que (proporcionan evidencia de que) los controles claves existen y que son aplicables en forma efectiva y uniforme.

Pruebas Sustantivas.- Son aquellas que implican el estudio y evaluación de la información, por medio de comparaciones con otros datos relevantes.

Resumen Ejecutivo.- Es un informe de fácil lectura, gramaticalmente correcto y breve, que presenta los hallazgos a la gerencia en forma comprensible.

Riesgo. Posibilidad de que no puedan prevenirse o detectarse errores o irregularidades importantes.

- ✓ **Riesgo inherente.** Existe un error que es significativo y se puede combinar con otros errores cuando no hay control.
- ✓ **Riego de control.** Error que no puede ser evitado o detectado oportunamente por el sistema de control interno.

- ✓ **Riesgo de detección.** Se realizan pruebas exitosas a partir de un procedimiento de prueba inadecuado.

Sistema Operativo: Software de sistema, es decir, un conjunto de programas de computadora, destinado a permitir una administración eficaz de sus recursos. Comienza a trabajar cuando es cargado en memoria por un programa específico, que se ejecuta al iniciar el equipo, o al iniciar una máquina virtual y, gestiona el hardware de la máquina desde los niveles más básicos, brindando una interfaz con el usuario.

Técnicas de auditoría. Métodos que el auditor emplea, para realizar las verificaciones planteadas en los programas de auditoría, que tienen como objetivo la obtención de evidencia.

UPS: Es un dispositivo que proveen y mantiene energía eléctrica de respaldo en caso de interrupciones eléctricas o eventualidades en la línea o acometida. Adicionalmente, los **UPS** cumplen la función de mejorar la calidad de la energía eléctrica que llega a las cargas, como el filtrado, protección de subidas (picos de tensión), bajadas de tensión (caídas), apagones y eliminación de corrientes parasitarias como ruidos, interrupción de energía, pérdida de data, etc.

RESUMEN

El presente trabajo, describe la Auditoría Informática de los Sistemas de Tecnología e Información, realizada a la Cooperativa de Ahorro y Crédito “Alianza del Valle”. Ltda. Utilizando COBIT, una herramienta desarrollada para, ayudar a los administradores de negocios a entender y administrar los riesgos asociados con la implementación de nuevas tecnologías, las buenas prácticas de COBIT están enfocadas en el ambiente de control óptimo que debe tener una empresa para de esta manera lograr una alineación efectiva entre TI y los objetivos de negocio. El fin de esta revisión técnica es identificar debilidades y emitir recomendaciones que permitan minimizar riesgos.

Para llevar a cabo la presente Auditoría, se realizaron las siguientes actividades:

- Entregar un listado de requerimientos a la entidad a ser auditada.
- Revisar la documentación entregada al Equipo de Auditoría.
- Se formularon preguntas, con el fin de aclarar ciertos puntos de la documentación.
- Se elaboraron encuestas al personal de la entidad.
- En base a los resultados obtenidos, se llevaron a cabo las entrevistas que constituye un método de auditoría personalizada, para profundizar en la indagación.
- Tomando como base las encuestas y las entrevistas, se elaboraron las pruebas sustantivas (checklist) y se recopilieron evidencias.
- De acuerdo a los resultados obtenidos en las encuestas, entrevistas y pruebas sustantivas y, alineando todos estos resultados con cada objetivo de control, que propone COBIT, se presentaron las observaciones y recomendaciones emitidas en un informe a la Gerencia.

PRÓLOGO

La naturaleza especializada de la auditoría de los sistemas de información y, las habilidades necesarias para llevar a cabo la misma, requieren el desarrollo, la generación y la promulgación de Normas Generales para la auditoría de los Sistemas de Información.

La auditoría de los sistemas de información se define como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes.

Para hacer una adecuada planeación de la auditoría en informática, hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características de área dentro del organismo a auditar, sus sistemas, organización y equipo.

En el capítulo 1 se detallan los objetivos y alcances del presente estudio, debidamente justificados, además se exponen algunos conceptos y parámetros que definen a la Auditoría Informática, relacionados con el ambiente de control, sus procesos y, los controles de TI.

El capítulo 2 indica el modelo COBIT, el cual es usado para este trabajo; describiendo los productos Cobit 4.0, sus generalidades, sus respectivos dominios y las ventajas sobre otros modelos.

En el capítulo 3 se presenta la Aplicación del Modelo en la Cooperativa de Ahorro y Crédito "Alianza del Valle".

En el capítulo 4 se presenta el informe y resultados del caso práctico, describiendo las debidas conclusiones y recomendaciones.

En el capítulo 5 se presentan las conclusiones y recomendaciones obtenidas a lo largo del presente trabajo.

CAPÍTULO I

AUDITORÍA INFORMÁTICA DE LOS SISTEMAS TECNOLÓGICOS DE INFORMACIÓN

1.1 GENERALIDADES

1.1.1 DESCRIPCIÓN GENERAL DEL PROYECTO

Antecedentes

Los Sistemas Informáticos, están integrados a la gestión empresarial; por ello, las normas y estándares informáticos deben estar alineados e implantados previa la aprobación de la Dirección de Sistemas de la organización, misma que se encargará de la implementación de controles de acceso a la información, que se maneja en los diversos procesos de la Cooperativa Alianza del Valle; en consecuencia, se debe destacar que, las organizaciones informáticas forman parte de la gestión de la empresa y se constituyen en un elemento de apoyo en la toma de decisiones.

Actualmente, la información institucional, se ha convertido en un activo fijo real invaluable, similar a la materia prima, sin embargo, debemos considerar que, a pesar de la capacidad que pueden tener los miembros de la Dirección de Sistemas de la Cooperativa Alianza del Valle; la cantidad de trabajo, centrado mayormente en el desarrollo de sistemas y redes, sin el personal suficiente hace que, necesariamente se tomen alternativas rápidas para ganar tiempo, afectando de esta manera, la calidad de los productos que se desean entregar, para servicio del cliente interno en este caso.

De ahí parte una necesidad de la Escuela Politécnica del Ejército, como parte del proceso de formación de profesionales en la Carrera de Ingeniería

en Sistemas e Informática, cooperando en el desarrollo del país, mediante la elaboración de tesis de grado, que certifiquen la formación de graduados, a la vez que colaboran con el desarrollo intelectual y personal en las empresas públicas y privadas y, el desarrollo constante del país.

1.1.2 JUSTIFICACIÓN E IMPORTANCIA

El desarrollo tecnológico que enfrenta la Cooperativa de Ahorro y Crédito “Alianza del Valle”, con el manejo de diversos sistemas de información y automatización en sus procesos, necesita corregir fallas, ejecutar procesos de calidad y, entregarlos en el momento oportuno; detectar los errores mediante una Auditoría Informática, realizada y ejecutada por un grupo capacitado, que proponga soluciones efectivas, para minimizar riesgos y mejorar el empleo de la tecnología de información en la organización.

La evaluación de los sistemas de información, deberá cubrir aspectos de planificación, organización, procesos, ejecución de proyectos, seguridades, equipos, redes y comunicaciones, con el objeto de determinar los riesgos a los que se encuentra expuesta la Cooperativa “Alianza del Valle” Ltda. y recomendar procedimientos que permitan minimizarlos o eliminarlos.

El análisis de los Objetivos de Control con COBIT¹, debe ser de carácter objetivo e independiente, crítico, basado en evidencias, sistemático, bajo normas y metodologías aprobadas a nivel internacional, que seleccione políticas, normas, prácticas, funciones, procesos, procedimientos e informes relacionados con los sistemas de información computarizados, que permiten obtener una opinión profesional e imparcial, enfocada en aspectos como: criterios de información y prácticas requeridas, que ayuden a determinar con

¹ Definición Informática por el Ingeniero Philippe Dreyfus

¹ Definición Informática: <http://www.mastermagazine.info/termino/5368.php>

¹ Definición Informática: <http://www.webtaller.com/maletin/articulos/que-es-informatica.php>

eficiencia, el uso de los recursos informáticos, la validez de la información y efectividad de los controles establecidos.

Como parte del sistema de administración de la Cooperativa Alianza del Valle, se hace evidente la necesidad de evaluar y valorar el uso de los recursos de TI, para de esta manera, justificar su costo y determinar medidas que permitan su racional aplicación, eficiencia y efectividad.

La situación actual por la que atraviesa la Dirección de Sistemas de la Cooperativa Alianza del Valle, requiere que, mediante el uso de un conjunto de procedimientos y técnicas, se proceda a evaluar y controlar los sistemas de información y el ambiente informático, con el fin de constatar si sus procesos y actividades son correctos y, se encuentran enmarcados y en conformidad con las mejores normativas informáticas y generales de la organización.

1.1.3 ALCANCE DEL PROYECTO

El presente proyecto de plan de tesis “AUDITORÍA INFORMÁTICA DE LA COOPERATIVA DE AHORRO Y CREDITO “ALIANZA DEL VALLE” LTDA”, está orientado a la revisión del control interno informático del Departamento de Sistemas de la Cooperativa de Ahorro y Crédito “Alianza del Valle”.

Se utilizará el estándar COBIT 4.0, para la evaluación y auditoría del ambiente informático de la Cooperativa de Ahorro y Crédito “Alianza del Valle” Ltda., profundizando conceptos de control interno y procedimientos que se ejecutan.

Los módulos en los que se ejecuta este proyecto, abarcan los siguientes aspectos:

- Identificación de Soluciones Automatizadas: donde se utilizaran criterios de información sobre efectividad y eficiencia en los procesos del

negocio, requeridos para la Cooperativa Alianza del Valle y, así satisfacer los requerimientos de los usuarios. Las prácticas de control que se utilizan en este módulo están directamente involucrados con los recursos de TI, siendo estos:

- ✓ Conocimiento de soluciones existentes en el mercado,
 - ✓ Metodologías de adquisición e implementación,
 - ✓ Involucramiento del usuario en el proceso de compra,
 - ✓ Orientación a las estrategias de TI y de la Cooperativa Alianza del Valle.
 - ✓ Definición de los requerimientos de información,
 - ✓ Estudios de factibilidad (costo, beneficio, alternativas, etc.),
 - ✓ Cumplimiento con la arquitectura de información,
 - ✓ Requerimientos de funcionalidad, operatividad, aceptación, sostenimiento y mantenimiento,
 - ✓ Seguridad y control de Costo-Beneficio,
 - ✓ Responsabilidad de los proveedores.
-
- Adquisición y Mantenimiento del Software de Aplicación: los criterios de información que se aplican, se enmarcan sobre parámetros de efectividad, eficiencia, integridad, cumplimiento y confiabilidad; llegando a proporcionar funciones automatizadas que soporten efectivamente los procesos del negocio y la especificación de los requerimientos funcionales y operacionales². Las prácticas de control que se aplican son:
 - ✓ Niveles de aceptación y pruebas funcionales,
 - ✓ Requerimientos de seguridad y controles de la aplicación,
 - ✓ Documentación requerida,
 - ✓ Ciclo de vida del software,
 - ✓ Arquitectura de la información empresarial,

- ² <http://www.auditoriasistemas.com/>

- ✓ Ciclo de vida metodológico para el desarrollo de aplicaciones,
 - ✓ Interface de usuario,
 - ✓ Personalización de paquetes.
- Adquisición y Mantenimiento de la Infraestructura Tecnológica: definidos sobre los criterios de información de efectividad, eficiencia e integridad, proveyendo al proceso de las plataformas apropiadas a las aplicaciones del negocio. La forma de lograrlo se dirige a una adquisición apropiada de hardware y software, estandarización de software y, un consistente sistema de administración. Las prácticas de control que se definen en esta etapa son:
 - ✓ Cumplimiento de las directrices y estándares de la infraestructura tecnológica,
 - ✓ Evaluación tecnológica,
 - ✓ Instalación, mantenimiento y control de cambios,
 - ✓ Actualizaciones, conversiones y, planes de migración,
 - ✓ El uso de infraestructura y/o recursos internos y externos,
 - ✓ Responsabilidades de los proveedores y la relación con los mismos,
 - ✓ Administración de cambios,
 - ✓ Costo total de propiedad,
 - ✓ Seguridad del software.
 - Desarrollo y Mantenimiento de Procesos: manejaremos algunos criterios de información, guiados sobre la efectividad, eficiencia, integridad, cumplimiento, confiabilidad; llegando a que el proceso del negocio asegure el uso apropiado de las aplicaciones y la infraestructura existente, con la sustentación de manuales estructurados de usuarios y operacionales, materiales de entrenamiento y requerimientos de servicio. Las prácticas de control son:
 - ✓ Rediseño de los procesos de negocio,
 - ✓ Consideración a los procedimientos como a cualquier otra tecnología existente,

- ✓ Desarrollo a tiempo,
- ✓ Procedimientos y controles de usuario,
- ✓ Procedimientos y controles operacionales,
- ✓ Materiales de entretenimiento,
- ✓ Administración de cambios.

Con el manejo apropiado de los recursos humanos, aplicaciones, tecnologías e instalaciones.

- Instalación y Acreditación de Sistemas: el proceso de negocio requerido sobre la verificación y confirmación de soluciones adecuadas, en base al propósito deseado y los criterios de información de efectividad, integridad y disponibilidad, con la realización de un plan formalizado de instalación migración y conversión. Las prácticas de control que se utilizan en este módulo se fusionan con los recursos de TI y, estas son:

- ✓ Entrenamiento de usuarios y del personal técnico de TI
- ✓ Conversión de Datos,
- ✓ Un ambiente de pruebas que refleje el ambiente real,
- ✓ Retroalimentación y revisiones post implementación,
- ✓ Participación del usuario final en la etapa de pruebas,
- ✓ Planes de continuo mejoramiento de calidad,
- ✓ Criterios y medidas de aceptación,
- ✓ Requerimientos continuos del negocio,
- ✓ Acuerdos y criterios de aceptación.

- Administración de Cambios: se encarga de la minimización de alteraciones, interrupciones y cambios no autorizados; manejando eficacia, eficiencia, integridad, disponibilidad y confiabilidad de un sistema de administración, que permita realizar una implementación, un seguimiento de todos los cambios requeridos y desarrollados a la infraestructura tecnológica actual. Algunas de las prácticas de control se describen a continuación:

- ✓ Identificación de cambios,
- ✓ Procedimientos de emergencia, categorización y priorización,

- ✓ Análisis de impacto,
- ✓ Autorización para cambios,
- ✓ Administración de versiones,
- ✓ Distribución de software,
- ✓ Uso de herramientas automatizadas,
- ✓ Administración de la configuración,
- ✓ Rediseño de los procesos del negocio.

El proyecto de tesis será ejecutado en el Departamento de Sistemas de La Cooperativa Alianza del Valle, ubicado en la ciudad de Sangolquí, para lo cual, se realizará la revisión de los controles mencionados con anterioridad y, establecidos en el proyecto del Departamento de Sistemas aplicando el estándar internacional COBIT 4.0.

1.1.4 OBJETIVOS

General

Realizar una Auditoría Informática del Sistema de Información de la Cooperativa Alianza del Valle, utilizando el estándar internacional COBIT 4.0, a fin de identificar debilidades y emitir recomendaciones que permitan eliminar o minimizar los riesgos en la organización.

Específicos

- Evaluar y describir la planeación, organización y situación actual de los Sistemas de Información de la Cooperativa Alianza del Valle, enfocándose en las estrategias, tácticas e infraestructura tecnológica de información, que contribuyen al logro de los objetivos del negocio.
- Evaluar la adquisición e implementación de las TI, los procesos en los que estas se desenvuelven, cambios y mantenimiento realizado a los sistemas existentes, así como la verificación de la calidad y suficiencia

de los procesos de la Institución y, el monitoreo de los requerimientos de control.

- Evaluar la entrega de los servicios requeridos, desde las operaciones tradicionales hasta el entrenamiento al personal que interfiere directamente con las Tecnologías de Información, abarcando aspectos de seguridad, continuidad del negocio, revisión del procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.
- Aplicar el estándar COBIT4.0 en la evaluación y auditoría de sistemas de la Cooperativa Alianza del Valle.
- Emitir recomendaciones que permitan asegurar una mayor integridad, confidencialidad y confiabilidad de la información, en base a un estudio y aplicación de metodologías, a los procesos de la Cooperativa Alianza del Valle.

1.1. AMBIENTE DE CONTROL

El ambiente de control se determina por el conjunto de circunstancias que enmarcan el accionar de una entidad, organización o empresa, desde una perspectiva de control interno y que son determinantes para el cumplimiento de las metas y objetivos de la organización en que los principios y políticas actúan, sobre las conductas y los procedimientos organizacionales.

El sistema de control interno está relacionado directamente con las actividades operativas y de procedimiento dentro de la organización y, existen por razones empresariales fundamentales y, a que estos fomentan la eficiencia, reducen el riesgo de pérdida de valor de los activos y, ayudan a garantizar la fiabilidad de los estados financieros y el cumplimiento de las leyes y normas vigentes.

El ambiente control se puede definir como un proceso, efectuado por el

personal de una organización, diseñado para conseguir objetivos específicos. La definición es amplia y cubre todos los aspectos de control de un negocio, pero al mismo tiempo, permite centrarse en objetivos específicos.

Los auditores deben considerar factores que influyen en la organización y que garantizan el éxito de sus procesos internos, siendo los más importantes los siguientes:

- La filosofía y el estilo de la dirección y gerencia.
- La estructura del plan organizacional, los reglamentos y los manuales de procedimientos.
- La integridad, los valores éticos, la competencia profesional y el compromiso de todos los colaboradores de la organización, así como su adhesión a las políticas y objetivos establecidos.
- Las formas de asignación de responsabilidades, de administración y desarrollo del personal.
- El grado de documentación de políticas, decisiones y de formulación de programas que contengan metas, objetivos e indicadores de rendimiento.

Cada uno de estos factores ayudan a que las organizaciones crezcan y cumplan sus principales objetivos, que permiten el éxito o fracaso de las mismas, siendo estos criterios:

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

De acuerdo a estos factores, es necesario realizar evaluaciones al ambiente de control que permitan identificar los riesgos y definir los controles adecuados para neutralizarlos, ya que el núcleo principal de control son las personas, mismas que, si no tienen una integridad probada, valores éticos y competencias, el resto de procesos posiblemente no funcionarán, por lo cual,

debe establecerse un adecuado ambiente de control sobre el que se desarrollan las operaciones de la organización evaluada.

1.2. EL PROCESO DE LA AUDITORÍA INFORMÁTICA

El proceso de la auditoría informática es similar al que se lleva a cabo a los de estados financieros, en el cual, los objetivos principales son: salvaguardar los activos, asegurar la integridad de los datos, la consecución de los objetivos gerenciales y, la utilización racional de los recursos, con eficiencia y eficacia, para lo que se realiza la recolección y evaluación de evidencias.

Para que una auditoría sea exitosa, debe tomar en cuenta muchos de los aspectos tratados en el punto anterior. A continuación se muestra un grafico que muestra cómo actúan conjuntamente todos los componentes, tanto de la empresa como del auditor, para que se genere una auditoría efectiva y eficaz.



Gráfica 1: Pirámide de procesos

Muchos de los componentes de la pirámide nacen de un proceso de auditoría, el cual se detalla a continuación y al cual hemos dividido en 3 etapas:

- Planificación de la auditoría Informática
- Ejecución de la auditoría Informática
- Finalización de la auditoría Informática

1.2.1. Planificación de la auditoría Informática

En esta fase se establecen las relaciones entre auditores y colaboradores de la organización, para determinar el alcance y objetivos. Se hace un bosquejo de la situación de la entidad, acerca de su organización, sistema contable, controles internos, estrategias y demás elementos que le permitan al auditor elaborar el programa de auditoría que se llevará a efecto.

Elementos Principales de esta Fase:

1. Conocimiento y Comprensión de la Entidad
2. Objetivos y Alcance de la auditoría
3. Análisis Preliminar del Control Interno
4. Análisis de los Riesgos
5. Planeación Específica de la auditoría
6. Elaboración de programas de Auditoría

1. Conocimiento y Comprensión de la Entidad a auditar.

Previo a la elaboración del plan de auditoría, se debe investigar y analizar todo lo relacionado con la entidad a auditar, para poder elaborar el plan en forma objetiva. Este análisis debe contemplar: su naturaleza operativa, su estructura organizacional, giro del negocio, capital, estatutos de constitución, disposiciones legales que la rigen, sistema contable que utiliza, volumen de sus ventas y, todo aquello que sirva para comprender exactamente cómo funciona la organización.

Para el logro del conocimiento y comprensión adecuados de la entidad, se deben establecer diferentes mecanismos o técnicas que el auditor deberá dominar, siendo entre otras:

- a) Visitas al lugar
- b) Entrevistas y encuestas
- c) Análisis comparativos de Estados Financieros
- d) Análisis FODA (Fortalezas, oportunidades, debilidades, amenazas)
- e) Análisis Causa-Efecto o Espina de Pescado
- f) Árbol de Objetivos.- Desdoblamiento de Complejidad.
- g) Árbol de Problemas

2. Objetivos y Alcance de la auditoría.

Los objetivos indican el propósito para el cual es contratada la firma de auditoría, qué se persigue con el examen, para qué y por qué. Si es con el objetivo de informar a la gerencia sobre el estado real de la empresa, o si es por cumplimiento de los estatutos que mandan efectuar auditorías anualmente, en todo caso, siempre se cumple con el objetivo de informar a los socios, a la gerencia y resto de interesados sobre la situación encontrada para que sirvan de base para la toma de decisiones.

El alcance de una auditoría ha de definir con precisión el entorno y los límites, en que va a desarrollarse la auditoría informática, se complementa con los objetivos de ésta.

Por otro lado, el alcance también puede estar referido al período a examinar: puede ser de un año, de un mes, de una semana y, podría ser hasta de varios años.

3. Análisis Preliminar del Control Interno

Este análisis es de vital importancia en esta etapa, porque de su resultado se comprenderá la naturaleza y extensión del plan de auditoría

y, la valoración y oportunidad de los procedimientos a utilizarse durante el examen.

4. Análisis de los Riesgos

El Riesgo en auditoría, representa la posibilidad de que el auditor exprese una opinión errada en su informe, debido a que los estados financieros o la información suministrada a él estén afectados por una distorsión material o normativa.

En auditoría se conocen tres tipos de riesgo: *Inherente*, de *Control* y de *Detección*.

El riesgo inherente, es la posibilidad de que existan errores significativos en la información auditada, al margen de la efectividad del control interno relacionado; son errores que no se pueden prever.

El riesgo de control, está relacionado con la posibilidad de que los controles internos imperantes no prevean o detecten fallas que se están dando en sus sistemas y que se pueden remediar con controles internos más efectivos.

El riesgo de detección, está relacionado con el trabajo del auditor y, es que éste en la utilización de los procedimientos de auditoría, no detecte errores en la información que le suministran.

La Materialidad es el error monetario máximo que puede existir en el saldo de una cuenta, sin dar lugar a que los estados financieros estén sustancialmente deformados. A la materialidad también se le conoce como Importancia Relativa.

5. Planeación Específica de la Auditoría.

Para cada auditoría que se va a practicar, se debe elaborar un plan. Esto lo contemplan las Normas para la ejecución. Este plan debe ser técnico

y administrativo. El plan administrativo debe contemplar todo lo referente a cálculos monetarios a cobrar, personal que conformarán los equipos de auditoría, horas hombres, etc.

6. Elaboración de Programa de Auditoría

Cada miembro del equipo de auditoría, debe tener en sus manos, el programa detallado de los objetivos y procedimientos de auditoría, objeto de su examen.

Ejemplo: si un auditor va a examinar el efectivo y otro va a examinar las cuentas por cobrar, cada uno debe tener los objetivos que se persiguen con el examen y los procedimientos que se corresponden para el logro de esos objetivos planteados.

Es decir, que debe haber un programa de auditoría para la auditoría del efectivo y un programa de auditoría para la auditoría de cuentas por cobrar y, así sucesivamente. De esto se deduce que un programa de auditoría debe contener dos aspectos fundamentales: Objetivos de la auditoría y Procedimientos a aplicar durante el examen de auditoría.

También se pueden elaborar programas de auditoría no por áreas específicas, sino por ciclos transaccionales.

1.2.2. Ejecución de la auditoría Informática

La ejecución de la auditoría informática, constituye la recopilación de la mayor cantidad de información necesaria, como son documentos y evidencias que permitan al auditor fundamentar sus comentarios, sugerencias y recomendaciones, con respecto al manejo y administración de TI.

Para la recolección de información, se pueden aplicar las siguientes técnicas:

- Entrevistas
- Simulación
- Cuestionarios
- Análisis de la información documental entregada por el auditado
- Revisión y Análisis de Estándares
- Revisión y Análisis de la información de auditorías anteriores

Toda la información entra luego en un proceso de análisis, el cual debe ser realizado utilizando un criterio profesional por parte de los auditores y el equipo a cargo del proceso de Auditoría, toda la información recopilada debe ser clasificada de manera que nos permita ubicarla fácilmente y además permita, luego del análisis respectivo, justificar de manera correcta las recomendaciones.

La evidencia se clasifica de la siguiente manera:

- a) Evidencia documental.
- b) Evidencia física.
- c) Evidencia analítica.
- d) Evidencia testimonial.

Una vez que tenemos información real y confiable, procedemos a evaluar y probar la manera en la que han sido diseñados los controles en la organización, para el mejoramiento continuo de la misma, para esto el equipo de Auditoría utilizara medios informáticos y electrónicos que permitan obtener resultados reales.

El equipo de auditores, para poder dar una opinión sobre un sistema o proceso informático, debe comprobar el funcionamiento de los sistemas

de aplicación y efectuar una revisión completa de los equipos de cómputo³.

1.2.3. Finalización de la auditoría Informática

Para finalizar un proceso de Auditoría Informática, se debe presentar un informe que contenga conclusiones y recomendaciones, necesarias para que una empresa este en mejoramiento continuo, esta documentación debe ser redactada por el equipo de Auditoría y entregarse a la Alta Dirección de la empresa para su evaluación y análisis.

Luego, en conjunto la Alta Dirección de la empresa y auditores, evaluarán los resultados del proceso; los auditores defenderán su punto de vista basándose en las evidencias recolectadas durante todo el proceso.

El informe que presenta el grupo de Auditores debe contener como obligatorios los siguientes puntos:

- Debe hacer constar el período de tiempo que abarcó la evaluación.
- Indicar el equipo de auditoría que intervino en la evaluación, se detallan los integrantes y su experiencia en el campo de auditoría.
- Indicar los objetivos que se propusieron alcanzar con el proceso de auditoría.
- También se debe indicar, en base a que se realizó la auditoría, en el caso de utilizar COBIT 4.0, se debe especificar el dominio que fue utilizado para la evaluación, esto debe especificarse claramente en el plan de trabajo que también debe ser entregado a la administración.
- Se debe indicar el criterio sobre el cual se está evaluando, en el caso de COBIT 4.0, lo más común es el de riesgos y el de objetivos de control.
- Se detalla la condición inicial en la que se encontró la empresa u organización.

³ Mckeever, J. "Sistemas de Información para la Gerencia", Editorial Mc Graw Hill, México (1984)

- Se describen las causas que generaron el diagnóstico inicial, además, se debe detallar las consecuencias que puede traer si la empresa continua manejándose de la misma forma.
- Detallar explicativamente las recomendaciones que se hacen a la Alta Dirección y qué medidas se deberían adoptar para poder cumplir con los objetivos propuestos desde el inicio y, la organización deje de ser afectada por circunstancias que fueron encontradas en la situación inicial.
- Dentro de los informes también incluye las opiniones y puntos de vista de la administración, debe especificarse si la organización va a adoptar o no las recomendaciones propuestas por el grupo de auditores.

El informe final se lo debe entregar a la Alta Dirección de la organización y como detallamos inicialmente, debemos presentar las evidencias de percances más importantes que se encontraron durante el proceso de Auditoría.

1.3. CLASIFICACIÓN DE LOS CONTROLES TI

Al momento de realizar un proyecto de auditoría, se desarrollan una gran variedad de actividades de control para verificar la exactitud, integridad y autorización de las transacciones. Estas actividades pueden agruparse en dos grandes conjuntos de controles de los sistemas de información, los cuales son: controles de aplicación y los controles generales de la computadora. Sin embargo, estos dos conjuntos de controles se encuentran estrechamente relacionados, puesto que, los controles generales de la computadora, son normalmente necesarios para soportar el funcionamiento de los controles de aplicación, además de la efectividad de ambos depende el aseguramiento del procesamiento completo y preciso de la información.

1.3.1. Controles de Aplicación

Los controles de aplicación son procedimientos manuales o automatizados que operan típicamente a nivel de los procesos de la organización. Los controles de aplicación pueden ser de naturaleza preventiva o de detección y están diseñados para asegurar la integridad de la información que se procesa en ellos. Debido a lo cual, los controles de aplicación se relacionan con los procedimientos utilizados para iniciar, registrar, procesar e informar las transacciones de la organización. Estas actividades de control ayudan a asegurar que las transacciones ocurridas, estén autorizadas y completamente registradas y procesadas con exactitud.

Debido al tamaño y complejidad de varios sistemas, no siempre se los podrá revisar a todos, por lo que es necesario evaluar los sistemas de aplicación para considerar en el plan de auditoría los sistemas de aplicación que tienen un efecto significativo en el desarrollo de las operaciones de la organización, con el fin de realizar un análisis más profundo de estos sistemas. Existen varios parámetros que se deben considerar para calificar los sistemas de aplicación, siendo los siguientes:

- Importancia de las transacciones procesadas.
- Potencial para el riesgo de error incrementado debido a fraude.
- Si el sistema sólo realiza funciones sencillas, como acumular o resumir información o funciones más complejas, como la iniciación y ejecución de transacciones.
- Tamaño y complejidad de los sistemas de aplicación.

Se debe incluir los controles implantados, para verificar la validez del ingreso de datos dentro de los sistemas, controles que podemos evaluar mediante el seguimiento manual de los informes de excepción o la corrección en el punto de entrada de datos. Debido al tamaño y complejidad de varios sistemas, no siempre se los podrá revisar a todos, por lo que es necesario evaluar los sistemas de aplicación para

considerar en el plan de auditoría aquellos que tienen un efecto significativo en el desarrollo de las operaciones de la organización, con el fin de realizar un análisis más profundo de estos sistemas.

1.3.2. Controles Generales

Los controles generales son políticas y procedimientos que se relacionan con muchos sistemas de aplicación y, soportan el funcionamiento eficaz de los controles de aplicación, ayudando a asegurar la operación continua y apropiada de los sistemas de información. Los controles generales mantienen la integridad de la información y la seguridad de los datos. Es por esto que antes de realizar una evaluación de los controles de aplicación, normalmente se actualiza la comprensión general de los controles del ambiente de procesamiento de la computadora y se emite una conclusión acerca de la eficacia de estos controles.

Las actividades que se llevan a cabo para la evaluación de estos controles, inician con entrevistas a la administración, luego de las cuales se tendrá una mejor capacidad para comprender y definir la estrategia y las pruebas que realizaremos sobre los controles. Posteriormente, se debe determinar si los controles generales de la computadora se diseñan e implementan para soportar el procesamiento confiable de la información, respecto a los controles que se han identificado, para lo cual se debe realizar lo siguiente:

- Evaluación del diseño de los controles, en la que se determinará que los controles evitan los riesgos para los que fueron diseñados.
- Determinar si los controles se han implementado, lo cual consiste en evaluar si los controles que se han diseñado y, se están utilizando durante el tiempo de funcionamiento de la organización.

CAPÍTULO II

Modelo COBIT 4.0

2.1. INTRODUCCIÓN

COBIT 4.0 tiene como misión desde sus inicios investigar, desarrollar, publicar y promover un conjunto de objetivos de control en tecnología de la información con autoridad, debidamente actualizados, de carácter internacional y aceptado generalmente para el uso cotidiano de gerentes de empresas y auditores.

Los gerentes, auditores y usuarios se benefician del desarrollo de COBIT 4.0 ya que este les ayuda a entender y comprender el nivel de seguridad de sus sistemas TI, además permite definir qué control es el necesario para proteger los activos de sus empresas mediante el desarrollo de un modelo de gobernación TI.

Los proyectos de auditoría Informática, necesitan de una base o estándar para guiarse; en el presente proyecto de tesis guiado, a la auditoría informática, se ha decidido tomar como base al Modelo COBIT versión 4.0 ya que permite un enfoque distinto y actual de los sistemas, por cuanto los mira en su ámbito global, formado por procesos manuales e informáticos.

Se adoptó la versión 4.0 del Modelo COBIT puesto que, una vez que se realizó un análisis de todas las versiones de COBIT se identificaron las siguientes características en cada una de ellas.

- Versión 1.0: uso de estándares internacionales, las pautas y la investigación en las mejores prácticas condujeron al desarrollo de los Objetivos del control.

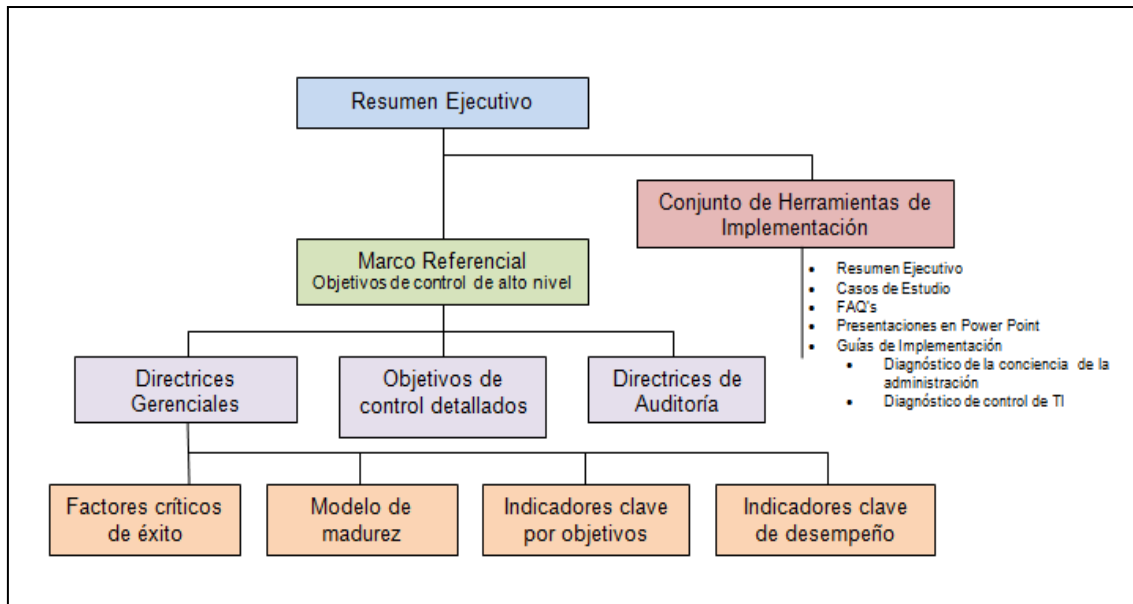
- Versión 2.0: análisis de fuentes internacionales, dedicados a la compilación, revisión e incorporación apropiada de los estándares técnicos internacionales, códigos de la conducta, estándares de calidad, estándares profesionales y los requisitos de la industria, como se relacionan con el marco y con los objetivos del control individual.
- Versión 3.0: consiste en proveer a la gerencia un uso del marco de referencia, COBIT, para que de él pueda determinar las mejores opciones a ser puestas en práctica y las mejoras del control sobre su información y tecnología relacionada.
- Versión 4.0: acentúa el cumplimiento regulator, ayuda a las organizaciones a aumentar el valor logrado de TI ya que posee un enfoque más gerencial que permite la alineación y simplifica la puesta en práctica del Modelo COBIT.
- Luego de este análisis se concluyó que la versión 4.0 se basa en los principios de, “proporcionar la información que la empresa requiere para lograr sus objetivos” y que “la empresa necesita administrar y controlar los recursos de TI, usando un conjunto estructurado de procesos que ofrezcan los servicios requeridos de información”⁴.

2.2. CONTENIDO (PRODUCTOS COBIT)

En el Modelo de COBIT 4.0 los productos se han definido en tres niveles, los mismos que dan soporte a:

- ✓ Administración y consejos ejecutivos.
- ✓ Administración del negocio y de Tecnología de Información.
- ✓ Profesionales de gobierno, aseguramiento, control y seguridad, como se detalla en la Gráfica 2.

⁴ GOVERNANCE INSTITUTE COBIT 4.0



Gráfica 2: Paquete de programas de COBIT

2.2.1. Resumen Ejecutivo

El Resumen Ejecutivo, consiste en una descripción que proporciona una conciencia cuidadosa y el entendimiento de los conceptos claves de COBIT, es decir, un entendimiento más detallado de los conceptos y principios de auditoría de Sistemas, identificando los cuatro dominios de COBIT y sus 34 procesos de TI.

2.2.2. Marco Referencial

El Marco Referencial COBIT, es la base para el desarrollo de los demás elementos COBIT. El marco referencial explica como los procesos de TI deben entregar la información, que el negocio requiere, para alcanzar sus objetivos, proporcionando al propietario de los procesos del negocio, herramientas que faciliten el cumplimiento de esta responsabilidad.

El Marco Referencial, permite también definir; si la información procesada para cumplir con los objetivos del negocio se están adaptando a los criterios de información (efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad), así como también define cuales de los recursos de TI (sistemas de aplicación, tecnología, instalaciones, datos) son importantes para apoyar a los objetivos del negocio.

2.2.3. Objetivos de Control

Un Objetivo de Control en TI, es la definición del resultado o propósito que se desea alcanzar siguiendo procedimientos de control específicos dentro de una Actividad de Control de TI. Los Objetivos de Control de COBIT son los requerimientos mínimos que debe cumplir un control de cada proceso de TI, para que sea definido como efectivo.

Los Objetivos de Control están definidos y orientados a los procesos, por medio del principio de reingeniería de negocios. Cada uno de los procesos de TI de COBIT tiene un objetivo de control de alto nivel y un número de objetivos de control detallados. A los que se les debe analizar como un todo ya que representan las características de un proceso bien administrado.

2.2.4. Guía o Directriz de Auditoría

Las Guías de Auditoría indican pautas y recomendaciones, mediante las que la gerencia de la entidad auditada puede cumplir de una manera más óptima con los Objetivos de Control.

Estas Guías de Auditoría provistas por COBIT no son específicas, sino son acciones genéricas que se pueden poner en práctica en mayor o menor grado, dependiendo de la entidad y están orientadas para proveer a la gerencia actividades que le permitan, mantener bajo control la información de la empresa y sus procesos relacionados, monitorear el

logro de las metas organizacionales, monitorear el desempeño de cada proceso de TI y llevar a cabo un benchmarking de los logros organizacionales.

2.2.5. Prácticas de Control

Las Prácticas de Control proveen guías para diseñar controles y cómo implementarlos, puesto que ayudan al personal encargado de diseñar e implementar controles específicos a administrar riesgos en proyectos de TI.

Además las Prácticas de Control ayudan a mejorar el rendimiento de TI ya que definen mejores prácticas para evitar el incumplimiento o mal uso de controles internos.

2.2.6. Guías de Administración

Las Guías de Administración o directrices gerenciales, contienen modelos de madurez asociado al gobierno de TI, que sirven para determinar en qué posición se encuentra la organización. También las Guías de Administración proveen factores críticos de éxito específico, indicadores claves por objetivo e indicadores clave de desempeño, que son las mejores prácticas administrativas para alcanzar los Objetivos de Control en TI.

2.2.7. Conjunto de Herramientas de Implementación

El Conjunto de Herramientas COBIT proporciona lecciones aprendidas por aquellas organizaciones que aplicaron COBIT, obteniendo resultados exitosos, las cuales pueden ser utilizadas por otras organizaciones.

Estas herramientas incluyen dos particularmente útiles:

- Diagnóstico de Sensibilización Gerencial (Management Awareness Diagnostic).
- Diagnóstico de Control en TI (IT Control Diagnostic), para proporcionar asistencia en el análisis del ambiente de control de TI en una organización.

2.3. GENERALIDADES DEL MODELO COBIT

2.3.1. Marco de Trabajo de COBIT

El modelo de COBIT fue creado para ser orientado a negocios y procesos, basado en controles e impulsado por mediciones.

2.3.1.1. Orientado a Negocios

El Modelo de COBIT es orientado a negocios ya que se encuentra diseñado para ser una guía para la gerencia, propietarios de los procesos de negocio, los proveedores de servicios, usuarios y auditores de TI. Además es el enfoque de control en TI que se lleva a cabo visualizando la información necesaria para dar soporte a los procesos del negocio. Siendo la Información el resultado de la aplicación combinada de recursos relacionados con la Tecnología de Información, que deben ser administrados por procesos TI.

El Marco de Trabajo de COBIT ofrece herramientas para garantizar la alineación de la administración de TI con los requerimientos del negocio, basados en los principios básicos de COBIT.



Gráfica 3: Principios básicos de Cobit

En donde los requerimientos de información del negocio, deben adaptarse a ciertos criterios de información, para que la misma permita cumplir con los objetivos de la organización, los cuales son:

- Efectividad: la información relevante y pertinente al proceso del negocio existe y es entregada a tiempo, correcta, consistente y utilizable.
- Eficiencia: es la optimización (más económica y productiva) de los recursos que se utilizan para la provisión de la información.
- Confidencialidad: es relativo a la protección de información sensitiva de acceso y divulgación no autorizada.
- Integridad: se refiere a lo exacto y completo de la información, así como a su validez de acuerdo con las expectativas del negocio.
- Disponibilidad: accesibilidad a la información para los procesos del negocio en el presente y en el futuro, también salvaguardar los recursos y capacidades asociadas a los mismos.
- Cumplimiento: son las leyes, regulaciones, acuerdos contractuales a los que el proceso del negocio está sujeto.
- Confiabilidad de la Información: proveer la información apropiada para que la administración tome las decisiones adecuadas para

manejar la empresa y cumplir con las responsabilidades de los reportes financieros.

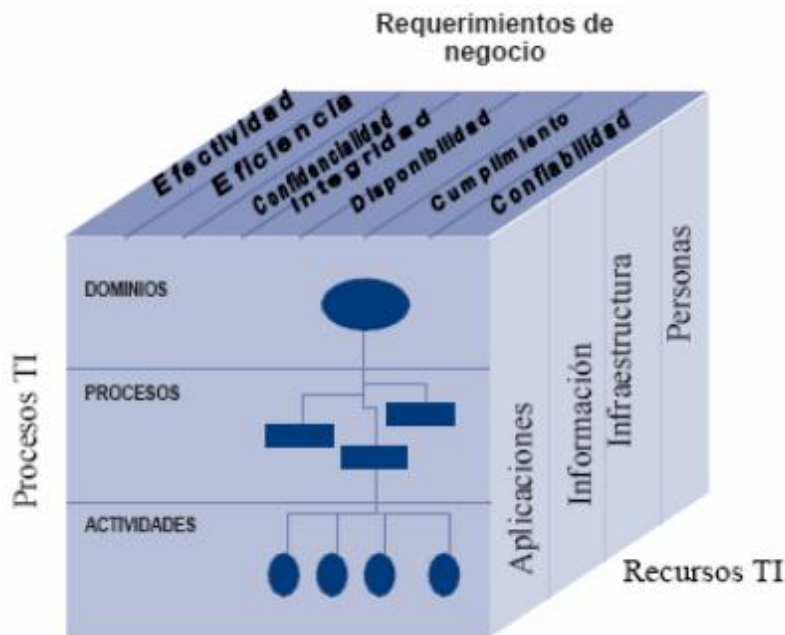
Una vez que las metas del negocio se encuentran alineadas y han sido definidas, requieren ser monitoreadas para garantizar que la entrega cumpla con las expectativas del negocio.

Los recursos de TI son:

- Datos: Todos los objetos de información interna y externa, estructurada o no, gráficas, sonidos, etc.
- Aplicaciones: los sistemas de información, que integran procedimientos manuales y sistematizados.
- Tecnología: incluye hardware y software básico, sistemas operativos, sistemas de administración de bases de datos, de redes, telecomunicaciones, multimedia, etc.
- Instalaciones: son recursos necesarios para alojar y dar soporte a los sistemas de información.
- Recursos Humanos: habilidad, conciencia y productividad del personal para planear, adquirir, prestar servicios, dar soporte y monitorear los sistemas de Información.

Se deben gestionar todos los recursos de TI, mediante un conjunto de procesos agrupados, para lograr metas de TI que proporcionen la información que el negocio necesita para alcanzar sus objetivos. Este es el principio básico del marco de trabajo COBIT, como se ilustra en el cubo COBIT⁵.

⁵ Definición Auditoría: <http://www.mega-consulting.com/herramientas/Auditoría/2concepto.htm>



Gráfica 4: Cubo cobit

2.3.1.2. Orientado a Procesos

Se pueden diferenciar tres niveles de actividades en un proceso de TI:

- El nivel superior de agrupación.- son los dominios que constituyen los procesos agrupados, los dominios en una estructura organizacional se denominan dominios de responsabilidad y se alinean con el ciclo de vida o administrativo de los procesos TI.
- En el nivel intermedio se encuentran los procesos, que son un conjunto de varias tareas y actividades.
- En el nivel bajo se hallan las actividades y tareas necesarias para alcanzar un resultado medible, es decir, son las actividades más discretas, como se puede observar en la Gráfica 5.



Gráfica 5: Niveles de actividades de ti

2.4. DOMINIOS

2.4.1. Planificación y Organización:

Cubre las estrategias, las tácticas y la manera de identificar la forma en que TI puede contribuir al logro de los objetivos del negocio.

2.4.1.1. Objetivos de Control Niveles Altos

Planificación y Organización

- PO1 Definen un Plan de TI Estratégico
- PO2 Definen la Información Arquitectura
- PO3 Determinan Dirección Tecnológica
- PO4 Definen los Procesos de TI, Organización y Relaciones
- PO5 Manejan la Inversión TI
- PO6 Comunican Objetivos de Dirección y Dirección
- PO7 Manejan Recursos TI Humanos
- PO8 Manejan Calidad

- PO9 Evalúan y Manejan Riesgos de TI
- PO10 Manejan Proyectos

2.4.2. Adquisición e Implementación

Cubre las estrategias de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como la implementación e integración en los procesos del negocio

2.4.2.1. Objetivos de Control Niveles Altos

- AI1 Identifican Soluciones Automatizadas
- AI2 Adquieren y Mantienen Software De aplicación
- AI3 Adquieren y Mantienen Infraestructura de Tecnología
- AI4 Permiten Operación y Usan
- AI5 Procuran Recursos TI
- AI6 Manejan Cambios
- AI7 Instalan y acreditan Soluciones y Cambios

2.4.3. Soporte y Servicios

Incluye los procesos de entrega o distribución, desde las operaciones tradicionales hasta el entrenamiento, tomando en cuenta aspectos de seguridad y continuidad de las operaciones. Con el fin de entregar servicios. En donde se incluye el procesamiento de datos, los sistemas de aplicación, clasificados de forma frecuente como controles de aplicación

2.4.3.1. Objetivos de Control Niveles Altos

Soporte y servicio

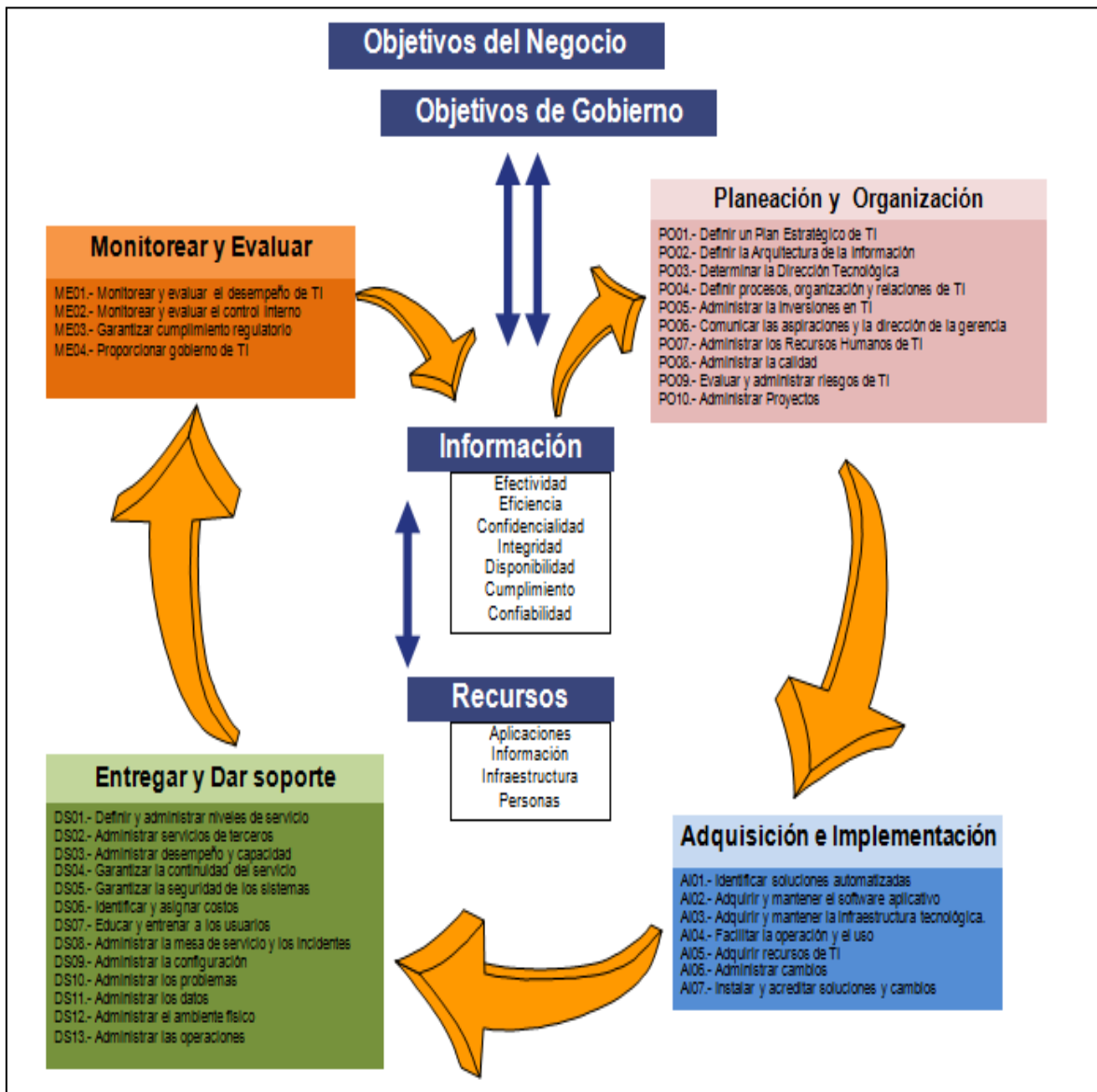
- DS1 Definen y Manejan Niveles de Servicio
- DS2 Manejan Servicios de Tercero
- DS3 Manejan Funcionamiento y Capacidad
- DS4 Aseguran Servicio Continuo
- DS5 Aseguran Seguridad de Sistemas
- DS6 Identifican y Asignan Gastos
- DS7 Educan y Entrenan a Usuarios
- DS8 Manejan Escritorio de Servicio e Incidentes
- DS9 Manejan la Configuración
- DS10 Manejan Problemas
- DS11 Manejan Datos
- DS12 Manejan el Ambiente Físico
- DS13 Manejan Operaciones

2.4.4. Evaluación y Seguimiento

Se debe evaluar de forma regular los procesos de control independientes, los mismos que son definidos por auditorías externas e internas o por fuentes alternativas. También abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno de TI.

2.4.4.1. Objetivos de Control Niveles Altos
Evaluación y seguimiento

- ME1 Supervisan y Evalúan Procesos de TI
- ME2 Supervisan y Evalúan Control Interno
- ME3 Aseguran Cumplimiento Regulatorio
- ME4 Proporcionan Gobernación TI



Gráfica 6: Marco de COBIT

2.5. VENTAJAS Y DESVENTAJAS SOBRE LOS MODELOS Y BUENAS PRÁCTICAS ITIL Y COSO

Tabla 1: Matriz Cobit vs Itil, Coso

| ATRIBUTO | COBIT | COSO | ITIL |
|--|---|---|---|
| Audiencia Primaria | Dirección, usuarios, auditores de SI | Dirección | Dirección, usuarios, auditores de SI |
| Objetivos Organizacionales del CI | Operaciones efectivas y eficientes Confidencialidad, integridad y disponibilidad de información Informes financieros confiables Cumplimiento de las leyes y regulaciones | Operaciones efectivas y eficientes Informes financieros confiables Cumplimiento de las leyes y regulaciones | Aplicar el ITIL en las empresas que han integrado en sus procesos a sus clientes y proveedores a través de redes informáticas. Ofrecer un marco común para todas las actividades del departamento de TI. |
| Componentes o Dominios | <u>Dominios:</u> Planeamiento y organización Adquisición e implementación Entrega y soporte Monitoreo | <u>Componente:</u> Supervisión Ambiente de control Administración de riesgos Actividades de control Información y comunicación | <u>Componentes (fases):</u> Estrategia del servicio Diseño del servicio Transición del servicio Operaciones del servicio Mejora continua del servicio |
| Foco | Tecnología Informática | Toda la entidad | Ciclo de vida de un servicio |
| Confiabilidad | Alta | Alta | Media |
| Tiempo que se requiere para su desarrollo | Depende de la disponibilidad de la información de las áreas de la empresa | Disponibilidad de la información | Depende del uso y del estado actual de la infraestructura TI |
| Costo | Alto | Alto | Alto |

| | | | |
|--|---|--|--|
| <p style="text-align: center;">VENTAJAS (CLIENTES Y USUARIOS)</p> | <p>Los usuarios finales obtienen una garantía sobre la seguridad y control de los productos que adquieren interna y externamente.</p> | <p>-Los usuarios de COSO son orientados sobre control interno, gestión del riesgo, fraudes, ética empresarial.</p> <p>-Confiability de la información financiera: control de la elaboración y publicación de estados contables confiables.</p> | <p>-Mejora la comunicación con los clientes y usuarios finales a través de los diversos puntos de contacto acordados.</p> <p>-Los servicios se detallan en lenguaje del cliente y con más detalles.</p> <p>-Se maneja mejor la calidad y los costos de los servicios.</p> <p>-La entrega de servicios se enfoca más al cliente, mejorando con ello la calidad de los mismos y relación entre el cliente y el departamento de IT.</p> <p>-Una mayor flexibilidad y adaptabilidad de los servicios</p> |
| <p style="text-align: center;">VENTAJAS (TI)</p> | <p>-Ayuda a salvar las brechas existentes entre riesgos de negocio, necesidades de control y aspectos técnicos.</p> <p>- Con el fin de proporcionar la información que la organización necesita para alcanzar sus objetivos, señala que los recursos de TI deben ser administrados por un</p> | <p>Las actividades de control: o las políticas, procedimientos y prácticas que aseguran el logro de los objetivos de la conducción y que se cumple con las estrategias para mitigar los riesgos</p> | <p>- La organización TI desarrolla una estructura más clara, se vuelve más eficaz y, se centra más en los objetivos de la organización.</p> <p>- La administración tiene un mayor control, se estandarizan e identifican los procedimientos y,</p> |

| | | | |
|--------------------|--|--|--|
| | <p>conjunto de procesos de TI agrupados en forma natural.</p> <ul style="list-style-type: none"> - Proporciona herramientas al responsable de los procesos que facilitan el cumplimiento de los procedimientos de TI. - Es la herramienta innovadora para el manejo de TI que ayuda a la gerencia a comprender y administrar los riesgos asociados con TI. | | <p>los cambios resultan más fáciles de manejar.</p> <ul style="list-style-type: none"> -La estructura de procesos en IT proporciona un marco para concretar de manera más adecuada los servicios de outsourcing. -A través de las mejores prácticas de ITIL se apoya al cambio en la cultura de TI y su orientación hacia el servicio y, se facilita la introducción de un sistema de administración de calidad. - ITIL proporciona un marco de referencia uniforme para la comunicación interna y con proveedores. |
| DESVENTAJAS | <ul style="list-style-type: none"> -Requiere cierto nivel de manejo de las TI, por lo que acoplarlo resulta ser un proceso, en cierto modo, más complejo que su propia ejecución. -COBIT consta con una cláusula de limitación de responsabilidad la cual obliga a los gerentes y | <ul style="list-style-type: none"> -Errores por falta de capacidad para ejecutar las instrucciones -Errores de juicio en la toma de decisiones. -Errores por mala interpretación, negligencia, distracción o fatiga. Inobservancia gerencial | <ul style="list-style-type: none"> -Tiempo y esfuerzo necesario para su implementación. - No se da un cambio previo en la cultura del área involucrada. - No se ve reflejada una mejora por falta de entendimiento |

| | | | |
|--|---|--|--|
| | <p>personas involucradas a investigar el manual de COBIT.</p> <p>-Resulta un modelo ambicioso que requiere de profundidad en el estudio.</p> <p>-No existe en la bibliografía de resultados experiencias prácticas de implementación de este modelo que lo hagan medible, para saber su nivel de confiabilidad.</p> | <p>a las políticas o procedimientos prescritos.</p> <p>-Colusión.</p> <p>-Costo - beneficio.</p> | <p>sobre procesos, indicadores y métodos para ser controlados.</p> <p>- El personal no se involucra y no se compromete.</p> <p>- La mejora del servicio y la reducción de costos puede no ser visible.</p> <p>- La inversión en herramientas de soporte sea escasa.</p> <p>Los procesos podrán parecer inútiles y no se alcanzaría las mejoras en los servicios.</p> |
|--|---|--|--|

CAPÍTULO III

Estudio del modelo COBIT en la Cooperativa de Ahorro y Crédito “Alianza del Valle”

3.1. SITUACIÓN ACTUAL DE LA ENTIDAD

Cooperativa Alianza del Valle, es una Institución que nació hace 41 años con el fin de colaborar con el progreso y bienestar de la comunidad y, es gracias a sus asociados que ha logrado convertirse en una institución financiera sólida con visión de liderazgo.

Alianza del Valle es una entidad solidaria que trabaja por la comunidad ofreciendo sobre todo seguridad y confianza, que le han convertido en Su Cooperativa Amiga.

Misión: “Satisfacer las necesidades y expectativas de nuestros socios, ofreciéndoles productos y servicios financieros innovadores, de calidad y con valor agregado, contando con una estructura administrativa/financiera sólida y con personal y directivos con visión social”

Visión: “Mantenernos como una Institución Financiera Sólida, con mayor participación en el mercado, que brinda productos y servicios financieros competitivos con cobertura nacional, para impulsar el desarrollo de los socios y de la comunidad con responsabilidad social.

Valores de la Cooperativa

Equidad: A través de un ambiente de justicia y transparencia para el otorgamiento de productos y servicios a nuestros socios/clientes, proveedores, entes de control y talento humano.

Honestidad: Con los asociados, recursos financieros, documentos, que sean de la Cooperativa, éstos serán utilizados con absoluta rectitud e

integridad organizacional. Trabajamos con transparencia y ética cuidando siempre el bienestar de nuestros socios e Institución.

Responsabilidad: Para asumir nuestras acciones, estando siempre preparados a esclarecer e informar sobre las actividades ejecutadas, de manera que el socio/cliente incremente su confianza en la capacidad del personal y de la Cooperativa como Institución sólida y transparente.

Disciplina: Cumpliendo a cabalidad normas, políticas y procedimientos que constituyen los pilares del accionar de la Cooperativa.

Solidaridad: Hacia nuestros socios/clientes y la comunidad ecuatoriana, basándonos en nuestros principios de ayuda mutua.

3.1.1. Conocimiento y comprensión de la institución.

La Cooperativa de Ahorro y Crédito “ALIANZA DEL VALLE” Ltda. Cuenta con los siguientes servicios:

Cooperativa en Línea, Contactos, Productos y Servicios, Cobertura.

Los productos y servicios que brinda la Cooperativa de Ahorro y Crédito “ALIANZA DEL VALLE” Ltda. Son:

Servicios:

- Seguro Amigo
- Tarjeta de Débito
- Pago de Bono de Desarrollo Humano
- Sistema de Remesas CREER Ecuador
- Impuesto Predial
- Sistema de Envíos Western Union
- Transferencias Interbancarias
- Megared - Ventanillas Extendidas
- Cpyline - Acreditaciones a Instituciones
- Acreditaciones IESS

Productos:

- Productos de Ahorro
 - Cuenta Efectiva
 - Cuenta Sueña
 - Cuenta Joven
 - Cuenta Metahorro

- Productos de Crédito
 - Seguro de desgravamen
 - Bajas tasas de interés
 - Cero comisiones
 - CrediConsumo
 - MicroCrédito
 - CrediVivienda

- Inversiones
 - Plazo Fijo Alianza

3.1.2. Conocimiento y comprensión de las actividades del departamento de TI.

El Departamento de TI tiene a su cargo las siguientes actividades principales:

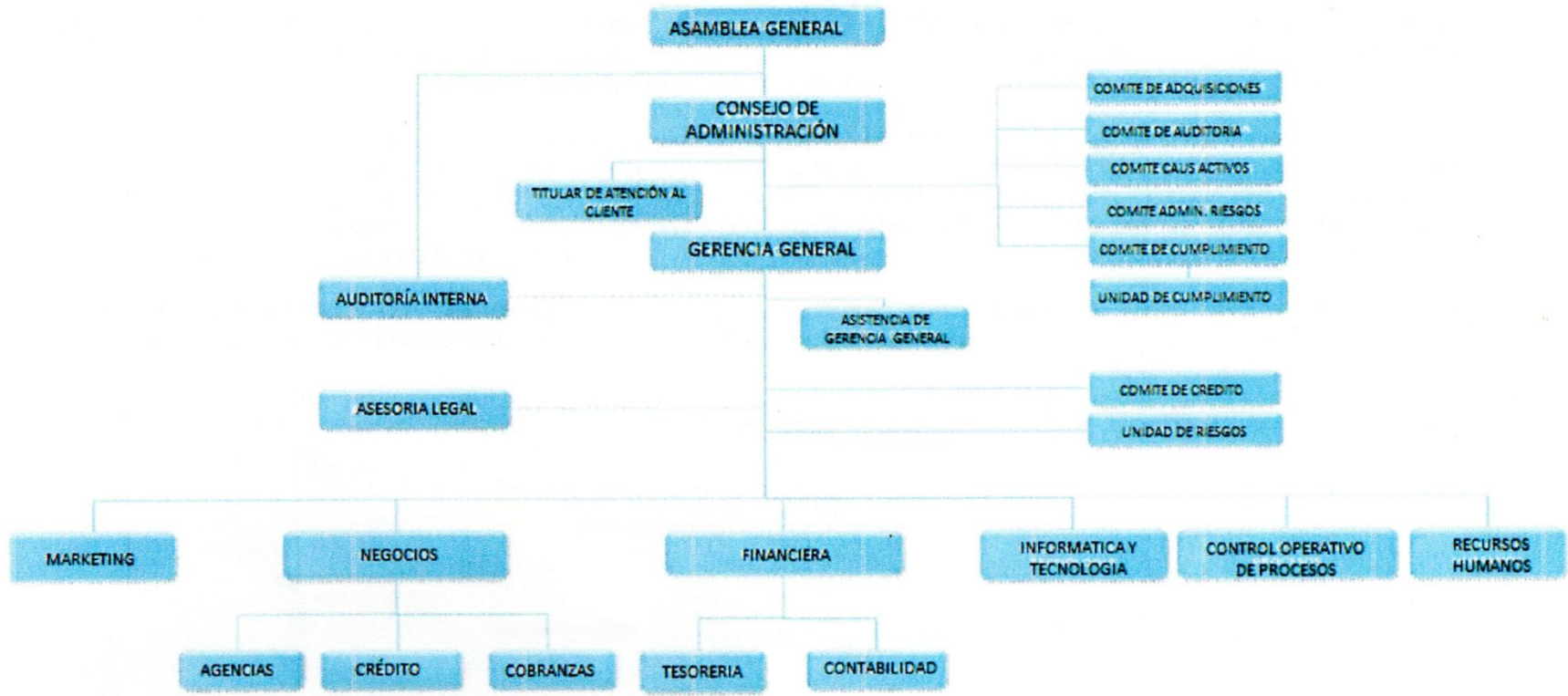
- Asesorar en el desarrollo e implementación de nuevas herramientas informáticas, que sirvan de instrumento para agilizar, simplificar, mejorar el desempeño de las actividades de los usuarios operativos y administrativos, salvaguardando la integridad, confiabilidad y disponibilidad de la información de la cooperativa.
- Apoyar, computacionalmente, las actividades de todos las Direcciones, Departamentos y otras unidades de la “Cooperativa

de Ahorro y Crédito “Alianza del Valle””, preocupándose del desarrollo de programas como de la actualización de todo su equipo.

- Mantener y administrar las redes, sistemas y equipos computacionales de la “Cooperativa de Ahorro y Crédito “Alianza del Valle””.
- Prestar soporte a usuarios en todo lo relativo a la plataforma computacional de la “Cooperativa de Ahorro y Crédito “Alianza del Valle””.
- Controlar las concesiones que le correspondan, de acuerdo a su participación, en la elaboración de las especificaciones técnicas y que le sean atinentes a la naturaleza de sus funciones.
- Velar por la integridad de la información almacenada en equipos computacionales, de propiedad de la cooperativa, además de elaborar y ejecutar los planes de contingencia necesarios en caso de pérdida de dicha información.
- Coordinar el accionar de las distintas dependencias de la “Cooperativa de Ahorro y Crédito “Alianza del Valle”” de manera de ir integrando y correlacionando información y bases de datos.
- Participar en la elaboración y ejecución del Plan Estratégico de la cooperativa; así como elaborar y ejecutar el Plan Anual Operativo del Departamento de TI.
- Proponer al Directorio para su aprobación, por medio del Área de Administración y de la Gerencia General, las políticas respecto a las Tecnologías de Información.

- Velar por la alta disponibilidad del Servicio de tecnología de Información que soporte la operatividad de la cooperativa.
- Proponer los planes y presupuestos para la adquisición de recursos de tecnologías de información, requeridos para asegurar la renovación tecnológica e implantación de los proyectos de Tecnología de Información.
- Establecer las normas y estándares para la gestión de las actividades y uso de recursos de tecnologías de información.
- Dar conformidad al cumplimiento de los contratos que deriven de la adquisición, alquiler y/o mantenimiento de equipos y/o aplicativos, dentro del ámbito de su competencia.
- Apoyar, dentro del ámbito de su competencia, en la definición de especificaciones técnicas de procesos de selección que guarden relación con tecnología de la información.
- Participar en la elaboración del Plan de Seguridad de la Información y el Plan de Continuidad de Negocios de la cooperativa, ejecutándolos de acuerdo al ámbito de su competencia.
- Hacer seguimiento del cumplimiento de los contratos de servicios solicitados por el área a su cargo.
- Atender e implementar las medidas correctivas, recomendadas por el Departamento de Auditoría Interna y los organismos de control externo.

3.1.3. Descripción de Funciones del nivel directivo



Gráfica 7: ESTRUCTURA ORGANIZACIONAL

La Estructura Organizacional de la Cooperativa de Ahorro y Crédito “Alianza del Valle” Ltda., está conformada por áreas, grupos y cargos ocupacionales

– **Áreas Ocupacionales**

Estos son conjuntos de actividades afines que constituyen las relaciones laborales

| AREA OCUPACIONAL |
|------------------|
| Directorio |
| Gerencia |
| Asesoría |
| Negocios |
| Apoyo |
| Control |

Gráfica 8: Área ocupacional

– **Grupos Ocupacionales**

Son ocupaciones de naturaleza similar, de acuerdo al tipo de funciones, responsabilidades y requerimientos para el cumplimiento de su ocupación.

| GRUPO OCUPACIONAL |
|------------------------------|
| Asamblea General |
| Consejo de Administración |
| Comités Técnicos |
| Gerencia General |
| Asesoría Legal |
| Auditoría Interna |
| Unidad de Riesgos |
| Unidad de Cumplimiento |
| Negocios |
| Agencias |
| Crédito |
| Cobranzas |
| Marketing |
| Finanzas |
| Contabilidad |
| Tesorería |
| Informática y Tecnología |
| Control Operativo y Procesos |
| Recursos Humanos |

Gráfica 9: Grupo Ocupacional

– **Cargos**

- Listado de Cargos

| OCUPACIONES |
|-------------------------------------|
| Gerente General |
| Auditor Interno |
| Asesor Legal |
| Jefe de Riesgos |
| Oficial de Cumplimiento |
| Titular de Atención al Cliente |
| Asistente de Gerencia |
| Auxiliar de Servicios Generales |
| Mensajero |
| Jefe de Negocios |
| Jefe de Crédito |
| Jefe de Cobranzas |
| Jefe de Agencia |
| Asistente de Negocios |
| Oficial de Crédito |
| Asistente de Crédito |
| Asistente de Balcón de Servicios |
| Recibidor Pagador |
| Notificador |
| Operador Call Center |
| Jefe Financiero |
| Tesorero General |
| Contador General |
| Asistente Contable |
| Jefe de Operaciones y Procesos |
| Oficial de Procesos |
| Oficial de Operaciones |
| Asistente de Operaciones |
| Jefe de Recursos Humanos |
| Jefe de Marketing |
| Jefe de Informática y Tecnología |
| Administrador de TI |
| Analista Programador |
| Programador |
| Administrador del Centro de Computo |
| Analista de Producción |

Gráfica 10: Ocupaciones

A continuación se describirá las principales funciones del personal relevante de la Cooperativa de Ahorro y Crédito “ALIANZA DEL VALLE” Ltda.

– Gerente General

- Presentar para aprobación del consejo de administración el plan estratégico, el plan operativo y el presupuesto de la cooperativa.
- Representar judicialmente a la cooperativa
- Responder por la gestión administrativa y financiera de la cooperativa
- Cumplir y hacer cumplir a los socios las disposiciones emanadas de la asamblea general y del consejo de administración
- Actualizar y mantener bajo custodia los inventarios de bienes y valores de la entidad.
- Contratar, remover y sancionar, de acuerdo a las políticas que fije el consejo de administración a los empleados de la cooperativa, cuyo nombramiento o remoción no sea de competencia de otro órgano de la entidad y fijar sus remuneraciones que deberán constar en el presupuesto de la entidad
- Suministrar la información que solicite los socios, representantes, órganos internos y su impacto en el patrimonio, cumplimiento del plan estratégico y sobre todo que sean solicitados, así como el plan anual de gestión.
- Informar al consejo de administración sobre la situación financiera de la entidad, de riesgos y su impacto en el patrimonio, cumplimiento del plan estratégico y sobre otros que sean solicitados, así como el informe anual de gestión.
- Mantener los controles y procedimientos adecuados para asegurar el control interno.
- Delegar o revocar delegaciones conferidas a otros funcionarios de la cooperativa, previa información al consejo de administración, sin que ello implique exonerarse de la responsabilidad legal.
- Presidir el comité de crédito de la cooperativa y los que determinen las normas de la junta bancaria

- Mantener y actualizar el registro de certificados de aportación
 - Ejecutar las políticas de tasas de interés y de servicios de acuerdo a los lineamientos fijados por el consejo de administración
 - Analizar y aprobar las estrategias de mercadeo de productos y servicios de la cooperativa
 - Evaluar los resultados de la implantación de las estrategias, según programa aprobado.
 - Aprobar la adquisición de bienes y servicios requeridos para la gestión de la cooperativa de acuerdo a lo establecido en el manual de adquisición
 - Suscribir convenios de préstamo con entidades financieras según políticas de endeudamiento aprobadas.
- Asistente de Gerencia
- Coordinar la agenda de Gerencia General
 - Elaborar memorandos y oficios para funcionarios, organismos de control, instituciones financieras y otros.
 - Cumplir actividades de apoyo administrativo a jefaturas de la cooperativa.
 - Asistir y coordinar reuniones de trabajo con jefes departamentales jefes de agencias, etc.
 - Monitorear el cumplimiento de instructivos, disposiciones, registros, reportes y mas requerimientos establecidos por las autoridades de la cooperativa y organismos de control.
 - Elaborar informes para el consejo de administración de las actividades realizadas por gerencial general.
 - Custodiar y velar por la correcta utilización de la central telefónica.
 - Supervisar el cumplimiento de entrega y recepción de correspondencia.
 - Administrar el programa de desbloqueo de claves de los funcionarios y empleados.
 - Administrar el módulo de seguridad de módulo COBIS
 - Realizar las veces de oficial de cumplimiento Back UP

– Auditor Interno

- Vigilar cualquier tiempo las operaciones de la institución
- Comprobar la existencia y el adecuado funcionamiento de los sistemas del control interno, con el propósito de proveer una garantía razonable en cuanto al logro de los objetivos de la institución; eficiencia y eficacia de las operaciones; salvaguarda de los activos; una adecuada revelación de los estados financieros; y, cumplimiento de las políticas y procedimientos internos, leyes y normas aplicables.
- Evaluar los recursos informáticos y sistemas de información de la institución del sistema financiero, con el fin de determinar si son adecuados para proporcionar a la administración y demás áreas de la institución, información oportuna y suficiente que cuenten con todas las seguridades necesarias.
- Verificar si la información que utiliza internamente la institución para la toma de decisiones y la que reporta a la superintendencia de bancos y seguridades es fidedigna, oportuna y surge de sistemas de información y bases de datos institucionales.
- Verificar que el director o el organismos que haga sus veces de la institución del sistema financiero haya expedido las políticas para prevenir el lavado de activos provenientes de actividades ilícitas y constatar la aplicación de estas por parte de la administración de la entidad controlada.
- Evaluar si la gestión del oficial de cumplimiento se sujeta a las disposiciones
- Verificar que la institución cuente con organigramas estructurales y funcionales;
- Verificar que la institución del sistema financiero cuente con un plan estratégico y que su formulación se efectuó a base de un análisis de elementos tales como: debilidades, oportunidades fortalezas y amenazas, líneas de negocios, mercado objetivo, evolución de la cuota de mercadeo, proyecciones financieras, planes de expansión o reducción, entre otros.

- Verificar la existencia, actualización, difusión, eficacia y, cumplimiento de las políticas, procedimientos, estrategias, metodologías formalmente establecidas para identificar, evaluar, controlar y administrar los riesgos y si estas son compatibles con el volumen y complejidad de las transacciones.
- Aplicar las pruebas de auditoría necesarias para verificar la razonabilidad de los estados financieros, la existencia de respaldos de los registros contables; y cumplimiento de las normas de carácter general dispuestas por la superintendencia de bancos y seguros contenidas en el catálogo único de cuentas y en la codificación de resoluciones de la superintendencia de bancos y seguros y de la junta bancaria.
- Evaluar la correcta selección y aplicación de los principios contables en la elaboración de los estados financieros
- Verificar la transparencia, consistencia, confiabilidad y suficiencia de las cifras contenidas en los estados financieros y de sus notas.
- Identificar las operaciones con partes vinculadas y verificar su adecuada revelación en los estados financieros para el caso de las cooperativas de ahorro y crédito que realizan intermediación financiera con el público y de las asociaciones mutualistas de ahorro y crédito para la vivienda.
- Suscribir conjuntamente con el representante legal y el contador general de la institución del sistema financiero, los estados financieros y demás reportes que se remitirán a la superintendencia de bancos y seguros.
- Verificar la suficiencia de los asientos contables incluidos en los estados financieros de la institución del sistema financiero, mediante la evaluación de los procedimientos aplicados por la administración y los auditores externos.
- Verificar que la institución del sistema financiero acate las disposiciones de la superintendencia de bancos y seguros, así como las recomendaciones de los auditores externos y del anterior auditor interno, si lo hubiese.

- Velar por el cumplimiento de las resoluciones de la junta general de accionistas, asamblea de socios, del director o de los órganos que hagan a sus veces, según corresponda.
 - Verificar que los aumentos de capital de la institución se ajusten a lo previsto en el artículo 42 de la ley general instituciones del sistema financiero y a las normas pertinentes de la codificación de resoluciones de la superintendencia de bancos y seguros y de la junta bancaria.
 - Elaborar el plan anual de auditoría a ser ejecutado durante el ejercicio económico y remitido a la superintendencia de bancos y seguros, en el formato establecido para ello.
 - Ejecutar el plan de auditoría, en base de los requerimientos de los controles establecidos.
 - Dirigir y coordinar las acciones de auditoría en las diferentes áreas, de acuerdo al plan aprobado.
 - Asesorar a gerencia general y jefaturas departamentales y de agencias.
- Jefe de Informática y Tecnología
- Administrar los recursos de informáticos y tecnológicos de la cooperativa.
 - Realizar el Plan estratégico y operativo del área alineando al plan estratégico institucional.
 - Elaborar presupuesto anual del departamento.
 - Elaborar o actualizar el plan de contingencia.
 - Planificación, seguimiento y monitoreo de los mantenimientos de las redes WAN, LAN (Remotas oficinas/locales) y del sistema COBIS, BDD (base de datos).
 - Instalación y configuración de software especializado
 - Asesorar a gerencia general de las nuevas herramientas informáticas.
 - Planificación, seguimiento y monitoreo de las actividades asignadas al área de TI y CC.

- Realizar un informe a gerencia general de la administración de los recursos informáticos y tecnológicos.
 - Planificación, seguimiento y monitoreo de los nuevos proyectos informáticos de software y hardware.
- Jefe de Riesgos
- Proponer al comité de administración integral de riesgos de la entidad, las políticas, de riesgos para la institución, de acuerdo con los lineamientos que fije el director u organismo que haga sus veces.
 - Elaborar y someter a consideración y aprobación del comité de administración integral de riesgos, la metodología para identificar, medir, controlar/mitigar y monitorear los diversos riesgos asumidos por la institución en sus operaciones.
 - Velar por el cumplimiento de los límites de explotaciones por tipo de riesgos respecto de los principales clientes, sectores económicos de actividad, área geográfica, entre otros.
 - Diseñar un sistema de información basado en reportes objetivos y oportunos, que permita analizar las posiciones para cada riesgo y el cumplimiento de los límites fijados; e, informar periódicamente al comité los planes de contingencia que considere distintas situaciones probables, según corresponda.
 - Implantar de manera sistemática en toda organización y en todos los niveles de personal las estrategias de comunicación, a fin de entender sus responsabilidades con respecto a la administración integral de riesgos.
 - Calcular las posiciones de riesgo y su afectación a patrimonio técnico de la entidad
 - Analizar la incursión de la institución del sistema financiero en nuevos negocios, operaciones y actividades acorde con la estrategia del negocio, con sujeción a las disposiciones legales, normativa y estatutaria, en cumplimiento del proceso de administración integral de riesgos.

- Analizar el entorno económico y de la industria y sus efectos en la posición de riesgos de la institución, así como las pérdidas potenciales que podrá sufrir ante una situación adversa en los mercados en los que opera.
- Diseñar las políticas y el proceso de administración del riesgo operativo.

3.1.4. Estructura Organizativa del Área de Sistemas



Gráfica 11: Estructura organizacional del área de sistemas

En la Cooperativa “Alianza del Valle” LTDA., al área tecnológica se la conoce como el Departamento de Tecnología e información, donde detallaremos los cargos principales que constituyen este departamento.

- .Administrador de TI: Administrar proyectos de software que satisfagan las necesidades de mejoramiento y calidad de los procedimientos y actividades institucionales, con la implementación de sistemas automatizados.

- Analizar los requerimientos enviados por el administrador de TI y apoyar en la mejora de estos.
- Administrador del Centro de Cómputo: Administrar los recursos tecnológicos monitoreando el buen desempeño de los equipos servidores, supervisar que las redes de telecomunicaciones estén operativas en su totalidad, controlar inventario del hardware y software licenciado.
- Operador: Ejecutar procesos diarios, mantener la operatividad de los equipos tecnológicos y servicios relacionados al área.
- Analista Programador: Analizar los requerimientos enviados por el administrador de ti y apoyar en la mejora de estos.
- Programador: Desarrollar software que cumpla con los requerimientos institucionales.

3.1.5. Características de los Sistemas y Ambiente Computarizado

3.1.5.1. COBIS Sistema Bancario

COBIS es un Sistema Bancario, que se encarga de manejar los siguientes módulos, que son fundamentales para el funcionamiento de la cooperativa:

- **MÓDULO DE CUENTAS DE AHORROS**

El módulo está diseñado para brindar un conjunto variado y completo de transacciones para la administración, manipulación y consultas sobre las cuentas de ahorros que posee el banco.

En lo que tiene que ver con el manejo de las libretas, el módulo presenta opciones para manipular las líneas pendientes, producto de la ejecución de transacciones internas o de transacciones en

las cuales el cliente no dispuso de la libreta (transacciones financieras sin libreta). Dicho manejo se ve complementado por las características que brinda la terminal financiera (ATX), para manejar diferentes tipos de impresoras validadoras y, con la operación de reimpresión, en caso de fallo en la impresión original, producto de la ejecución de una transacción con libreta.

ESTANDARES:

Cuentas de Ahorro

Personalización

Remesas

- **MÓDULO DE CARTERA**

Cobis Cartera, presenta una solución a los problemas que se presentan al procesar los préstamos, permitiendo tener un control total sobre cada una de las operaciones, realizando cálculos diarios de los valores que deben cobrarse por cada uno de los conceptos que se definen en un préstamo y teniéndolos disponibles el momento que se requiera. El módulo tiene una gran facilidad en cuanto a la simulación de tablas de amortización, la misma que facilitará la negociación de un crédito, proporcionando un mejor servicio al cliente y optimizando recursos de la empresa. También se encuentra diseñado para que pueda realizar procesos de regeneración de tablas de amortización por reajustes de tasas, lo cual ocasiona problemas y mucho esfuerzo para poder controlar correctamente si no existe un sistema automático. Permite aceptar cualquier tipo de abono que desee hacer el cliente con su correspondiente aplicación y registro.

- **MÓDULO CONTABIIDAD**

Manejo de Empresas

El módulo de Contabilidad permite el manejo multiempresa o manejo contable de diferentes empresas, asociándolas por tipos de planes, por grupos económicos o por su capacidad de manejo contable, independiente por empresa, ofreciendo servicios contables para empresas ajenas al grupo económico.

Manejo de la Estructura Organizacional

El sistema se adapta a la estructura de cada empresa, permitiendo definir la estructura organizacional de la misma (oficinas y áreas).

Se puede realizar consultas de todas las sucursales existentes en la empresa, o realizar una búsqueda de las mismas según su jerarquía o nombre.

Las áreas también pueden ser definidas como operativas o canceladas.

Periodos Contables

Es posible definir los periodos contables que el usuario requiera, con fechas de inicio y fin de los mismos. En consecuencia, es posible, por ejemplo, trabajar con un nuevo periodo (año 95) y seguir disponiendo del anterior periodo (año 94) para realizar ajustes y correcciones. También es posible realizar comparaciones de resultados generados por cada periodo. Los periodos pueden ser anuales, semestrales, mensuales, etc. Al finalizar un periodo contable se transfieren los saldos de las cuentas de resultados a utilidad o pérdida del

ejercicio, luego de lo cual éstas son inicializadas para el comienzo de un nuevo periodo.

Plan de Cuentas

Es posible definir un Plan de Cuentas para cada Empresa, sin límite en el número de niveles ni en el número de dígitos por nivel. Es posible definir qué cuentas son operativas en qué nivel organizacional.

El Plan de Cuentas se asocia a las diferentes oficinas y por cada una de las oficinas a las diferentes áreas, según como el usuario lo defina. Esta asociación se realiza de una manera fácil y dinámica, lo que permite tener un Plan de Cuentas completo por cada Empresa y dentro de la misma por cada nivel organizacional (región, sucursal o agencia), sin un crecimiento innecesario del plan de cuentas.

Manejo de Monedas

El sistema maneja múltiples tipos monedas, lo que permite obtener saldos en función de ellos.

Un archivo histórico de monedas extranjeras, permite conocer las cotizaciones tanto de compra como de venta, pudiéndose obtener gráficos históricos.

Uso de Comprobantes Contables

Los comprobantes tienen las siguientes características:

Las cuentas contables que intervienen en los comprobantes, deben ser digitadas con su respectivo dígito de verificación para evitar cualquier ingreso erróneo.

El módulo controla automáticamente el cuadro de débito contra el crédito.

El módulo genera el número de comprobante por departamento, e imprimir los comprobantes contables generados.

Es posible el manejo de entradas interiores, a través de las cuales se permite el cruce de valores monetarios entre oficinas o departamentos.

Recepción de comprobantes contables, desde el departamento de contabilidad, o desde todas las agencias y, de todos los productos bancarios de las agencias.

Saldos Contables

Es posible la consulta automática de saldos sumariados de la Empresa; saldos por Oficinas, por Sucursales, (Machachi, Guamaní, Amaguaña, Sangolquí, Inca, Conocoto, Ecuatoriana, Chillogallo, Matriz). y, de todas y cada una de las cuentas contables: es decir hasta el nivel estructural más bajo y profundo que se requiera.

Los saldos pueden ser obtenidos por oficina, periodo requerido y corte, pudiéndose obtener gráficos de la variación de saldos de la cuenta.

Reexpresión Monetaria

El sistema convierte todos los saldos en moneda extranjera, a la moneda base que se haya definido para la Empresa, para la presentación de Balances a la Superintendencia de Bancos.

Interfaces Contables

Manejo de interfaces contables con Productos Bancarios como: Cuentas Corrientes, Cuentas de Ahorros y Cámara y Remesas, etc., para la realización de transacciones, indicando los sucursales origen y destino de la transacción, así como la empresa a la que pertenecen dichas sucursales.

Control Presupuestario

Es posible el manejo del Control Presupuestario mensual, con partidas presupuestarias armadas, definiéndose las cuentas de Presupuesto (similares a las del Plan de Cuentas). Al final de cada periodo es posible hacer una comparación gráfica entre ambos sistemas de cuantías.

- **MÓDULO DE CRÉDITO**

El módulo de crédito, permite automatizar el proceso de concesión de crédito, facilitando la apertura de una solicitud de crédito (operaciones originales, renovaciones o líneas de crédito), el control y aprobación de las etapas de dicha solicitud, o su rechazo y, el seguimiento de los préstamos otorgados y rechazados por la Institución Financiera, brindando toda la información necesaria para la toma de decisiones oportunas con el menor riesgo para la Institución.

- **MÓDULO DE FIRMAS**

Mediante el presente módulo se pueden digitalizar firmas de clientes. También pueden digitalizarse sellos de compañías. El número de firmas y sellos que pueden ser registrados por cliente es virtualmente infinito. Para ello es necesario, además del presente módulo, de un *scanner* convenientemente conectado al equipo Cliente (tarjeta de *scanner*).

El módulo puede ser usado en diferentes niveles de operatividad, según se hayan definido los Roles por medio del módulo Administración y Control Distribuido; pero básicamente admitiría dos roles: aquel que permite registrar nuevas firmas de clientes (y necesarias actualizaciones), según se indica en el primer párrafo y, otro para la Administración de dichas firmas.

- **MÓDULO VALORES EN GARANTÍA**

El módulo está diseñado para brindar un conjunto variado y completo de transacciones, para la administración, manipulación y consultas sobre las garantías que posee la institución financiera.

El módulo de Valores en Garantías, registra la información de las garantías que presenta un cliente al momento que éste solicita una operación de Crédito. Complementariamente, presenta opciones para realizar el mantenimiento y consultas de las garantías, así como el manejo de las inspecciones realizadas a las garantías que las requieran.

- **MÓDULO CLIENTES**

El módulo de CLIENTES permite la simulación de condiciones operativas de una Institución, el análisis de nuevos productos y servicios considerando las características de los clientes, permitiendo su segmentación por mercados y ubicación geográfica.

El módulo consta de 3 elementos principales:

El CIF (Central Information File)

Que contiene la información general de los clientes de la institución, sus relaciones con otros clientes y con los productos bancarios y financieros que tienen contratados.

Información para Mercadeo

Manejo de información para soporte a las actividades del área de mercadeo de la Institución, con posibilidades de análisis de factibilidad de nuevos productos, distribución geográfica de clientes y evaluación del comportamiento de productos.

Información de Saldos de Clientes

Obtención de información sobre los Saldos, Saldos Promedios y Flujo de Movimientos por Cuentas Corrientes y Cuentas de Ahorro de cada Cliente o Grupo Económico en los últimos seis meses.

- **MÓDULO DEPOSITOS A PLAZO FIJO**

El sistema de información COBIS Depósito a Plazo Fijo, brinda al banco, la facilidad de poder controlar la gestión originada en el manejo de los diferentes tipos de depósitos que son utilizados por el mismo.

El control sobre los depósitos se inicia con el ingreso de éste al sistema, permitiendo registrar la información necesaria para poder realizar los procesos de cálculos de intereses, fecha de vencimiento, fecha de próximo pago, etc. apropiadamente.

El sistema se encuentra alojado en el servidor central de producción de la Cooperativa, en auditoría informática este sistema debe ser analizado en su comportamiento de motor transaccional basándose en algunos puntos claves como son:

- Configuración de permisos de acceso de comunicaciones
- Configuración del motor transaccional
- Conexión a la base de datos
- Variables de entorno en el sistema
- Revisión de estadísticas de ejecución de transacciones del sistema
- Comportamiento del sistema en el ambiente de producción

COBIS contiene dos componentes muy importantes para su funcionamiento como son el MUX y COMSERVER estos son utilizados con la finalidad de eliminar posibles cuellos de botella en el servidor central al responder las transacciones solicitadas por los servidores de agencia, en un instante específico o en caso de transacciones recursivas o masivas.

3.1.5.2. Base de Datos

La Cooperativa tiene a COBIS como su Core Bancario siendo su administrador de Base de Datos un Servidor Adaptive Server Enterprise de Sybase.

La Cooperativa cuenta con un plan de contingencia y continuidad del servidor de Base de Datos y tienen configurado el Sistema de Contingencia o Standby mediante la Recopilación Sybase.

Para el buen funcionamiento de la base y evitar pérdidas de información o caídas en la conexión el departamento de Sistemas asigna 2 procesadores y discos con la suficiente capacidad para soportar el número de transacciones diarias.

Los usuarios se conectan directamente a la base de datos.

A continuación se describe la arquitectura del Sistema de Base de Datos y Replicación.

3.1.5.3. Servidores

La Cooperativa cuenta con servidores (Branch) de Producción, un Servidor central y uno de Transacciones.

El servidor central es el que controla toda la información importante de la Cooperativa de Ahorro y Crédito “Alianza del Valle”, tanto de la matriz como sus agencias.

Los servidores Branch , se encuentran en cada una de las agencias, estos son los que se conectan directamente al central, mismo que se encuentra en la matriz, para el intercambio y actualización de información.

Cada servidor de agencia presenta lo siguiente:

- Posee configurado 4 APLSERVER(según la carga que soportan)
- Esquema de seguridad
- Encolamiento en las transacciones

| | |
|--------------------------------|---------------|
| Servidor de producción | |
| Nombre del host | Alianza |
| Dirección IP | 192.10.1.3 |
| Servidor de Standby | |
| Nombre del host | alianza1 |
| Dirección IP | 192.168.102.3 |
| Servidor de Replicación | |
| Nombre del host | Alianza |
| Dirección IP | 192.10.1.101 |

| Servidor de Base de Datos | |
|----------------------------------|-------------------------------------|
| Nombre del host | SERVIDOR ASE DE PRODUCCION |
| Dirección IP | 192.10.1.3 |
| Nombre del host | SERVIDOR ASE DE STANDBY |
| Dirección IP | 192.168.102.3 |
| Nombre del host | SERVIDOR ASE QUE ADMINISTRA LA RSSD |
| Dirección IP | 192.10.1.101 |

Gráfica 12: especificación de servidores

- Servidor Central Sun Fire 250 (**PRODUCCIÓN**)
- Servidor Central SUN 250 ENTER PRISE (**DESARROLLO**)
- Servidor Compaq EVO para control de BANRED
- Servidor HP de red LAN de Matriz Alianza de Valle
- Servidor HP Linux Firewall
- Servidor HP cajeros automáticos
- Servidor HP Sitio Web

3.1.5.4. Microsoft Visual Source Safe

Es una herramienta que dentro de la Cooperativa se utiliza para el control de acceso a los programas fuentes y ejecutables; cabe destacar que, solamente el personal del área de desarrollo tiene acceso de administrador, permitiéndoles tener todos los privilegios necesarios para poder realizar cambios sea en línea de código o configuración del sistema ejecutable.

Claro que para poder realizar cualquier cambio en el software, existe una política de administración, en la cual se debe especificar con que intención o beneficio se realiza el cambio.

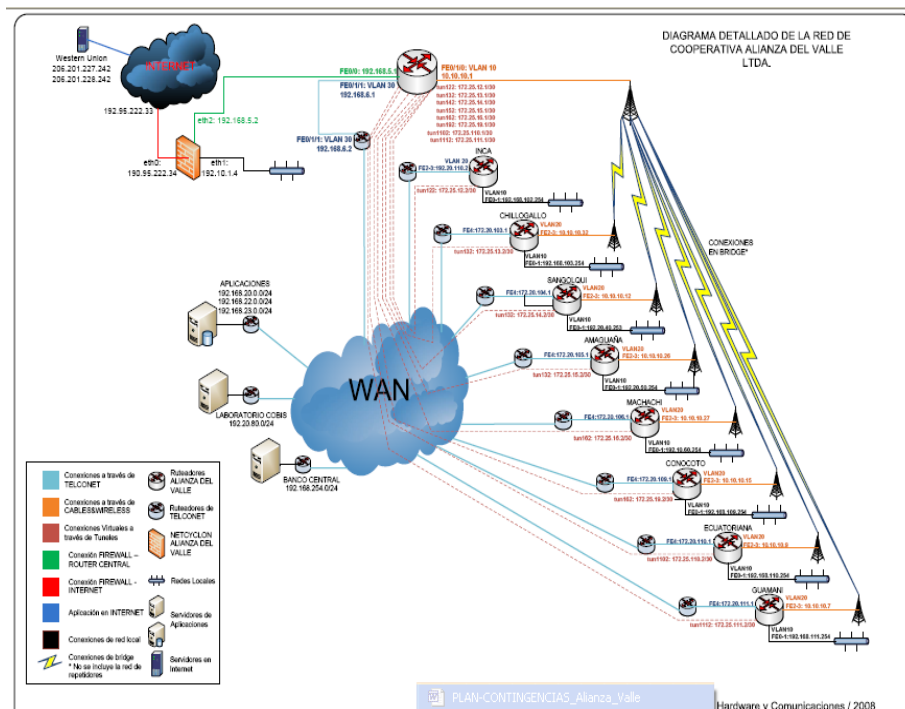
3.1.5.5. RED

Equipos de Comunicaciones cableado.-

Se compone de dos concentradores de red que se podrían denominar como principales, su red es plana, utilizando equipos de comunicaciones tales como.

El primero es un SWITCH 3COM de 24 y 12 Puertos a 100 MBPS que controla los puntos de red que desde el servidor están interconectados en un rack en la sala de máquinas del área de sistemas; desde este sitio se distribuye la red a todos los, para su gestión.

En cuanto a la distribución de los puntos de red, estos han sido realizados mediante cableado tipo par trenzado UTP categoría 5e, mismo que permite una transmisión entre 100 BT 100 MBPS y que se ha extendido bajo canaleta de plástico.



Gráfica 13: Esquema de la red LAN/ WAN

3.2.APLICACIÓN DEL MODELO COBIT, A LA COOPERATIVA DE AHORRO Y CREDITO “ALIANZA DEL VALLE”

3.2.1. Justificación de la Aplicación de los Dominios de Planear y Organizar y, Monitorear y Evaluar, del Modelo Cobit.

Para la realización de esta auditoría, se toma como marco de referencia COBIT 4.0, el cual es un marco de gobernabilidad de TI y un conjunto de herramientas de ayuda, que permite a los administradores, tener en cuenta y asociar los conceptos de requerimientos de control, consideraciones técnicas y riesgos del negocio.

Este conjunto de las mejores prácticas permiten evaluar la seguridad, eficacia, calidad y eficiencia de las TI., mediante esto se determinan los riesgos, tener una gestión efectiva de los recursos, medir el desempeño y cumplimiento de metas y, de manera principal, medir el nivel de madurez de los procesos de la organización.

COBIT satisface las necesidades que tiene la organización en lo referente a las TI de la siguiente manera:

- Tomando en cuenta los requerimientos del negocio.
- Mediante el modelo de procesos, organiza las actividades de TI.
- Identifica los recursos de TI prioritarios a ser utilizados.
- Definiendo los controles de TI.
- Garantizando la relación entre los Planes de Negocio y TI.
- Asegurando que TI entregue todos los beneficios pronosticados en la estrategia.
- Administrando los Recursos críticos.

- Medición del desempeño, monitoreando y rastreando la estrategia de implementación, el uso de recursos entre otros.

3.2.2. Planificación del Trabajo (propuesta)

3.2.2.1. Marco Teórico

La metodología a utilizarse en el proyecto es Cobit 4.0 (Control Objectives For Information an Related Technology), estándar generalmente aceptado para buenas prácticas en seguridad tecnológica y, en administración y control de la tecnología de la información.

Cobit tiene su base en los objetivos de control de ISACF, actualmente conocida como ISACA (Information Systems Audit and Control Association), de acuerdo a estándares internacionales, este modelo de referencia tiene la facilidad de adaptarse a cualquier tipo de negocio y, los objetivos de control que se han definido en el modelo, pueden ser aplicados independientemente del ambiente, plataformas y madurez tecnológica de la organización; por lo que se proyecta aplicar el Marco Referencial Cobit, adaptado a la Cooperativa de Ahorro y Crédito “Alianza del Valle” Ltda., que se sujeta a prácticas de administración a través de objetivos de control de “alto nivel”, organizadas en cuatro categorías o dominios.

- Planificación y organización.
- Adquisición e implementación.
- Soporte y servicios.
- Evaluación y seguimiento.

Cada uno de estos dominios contiene declaraciones de los resultados que se desean obtener, mediante la implementación de procedimientos de controles específicos y relacionados a la actividad

TI, en función de los riesgos identificados y focalizados en el Departamento de Recursos Informáticos de la COOP Alianza del Valle Ltda.

3.2.2.2. Objetivos

3.2.2.2.1. Objetivos Generales

Realizar una Auditoría Informática de los Sistemas de Información Tecnológicos de la Cooperativa de Ahorro y Crédito “Alianza del Valle LTDA”, en los dominios de “Planificación y organización, Adquisición e implementación, Soporte y servicios, Evaluación y seguimiento”, mediante la revisión del ambiente de control, implementado en los procesos automatizados y en el gerenciamiento de los mismos, utilizando COBIT, a fin de identificar debilidades y emitir recomendaciones que permitan eliminar o minimizar los riesgos.

3.2.2.2.2. Objetivos Específicos

- Presentar el marco teórico del Modelo Cobit 4.0.
- Evaluar la situación actual de la organización y su infraestructura tecnológica.
- Identificar la forma en que el uso adecuado de la tecnología de la información, puede contribuir al logro de los objetivos de la organización.
- Evaluar la eficiencia y eficacia con que los Sistemas de Información, apoyan en la toma de decisiones a la Alta Dirección de la organización, considerando el nivel de detalle provisto por los "Objetivos de Control" y las "Directrices de Administración" de Cobit, principalmente

enfocados en los criterios de efectividad, disponibilidad, confidencialidad e integridad.

3.2.2.3. Alcance

El alcance viene dado por la metodología COBIT, en los dominios de “Planificación y Organización” y, “Evaluación y Seguimiento”; que nos indica la forma de utilizar la tecnología de la información para lograr los objetivos del negocio; y su evaluación paulatina para verificar su calidad y suficiencia, en cuanto a los requerimientos de control.

Como primera actividad se espera recoger, agrupar y evaluar evidencias, para determinar si el sistema informático mantiene la integridad de los datos y, principalmente si lleva a cabo eficazmente los fines de la organización, utilizando eficientemente los recursos.

Este trabajo se ejecutará en la Cooperativa de Ahorro y crédito “Alianza del Valle LTDA”, para lo cual se realizará la revisión de controles establecidos dentro de la cooperativa, aplicando el modelo COBIT. El proyecto que tendrá una duración de 20 semanas, al final de las cuales se espera obtener recomendaciones en base a las falencias detectadas, las cuales nos permitirán generar recomendaciones que quedarán planteadas en el informe final para que puedan ser aplicadas según el criterio de las autoridades.

3.2.2.4. Método de Trabajo y Procedimientos a Ejecutar

Durante la auditoría, se debe recopilar información útil y necesaria, misma que luego analizarla, permiten obtener conclusiones, que luego derivan en recomendaciones para el mejoramiento de la organización. La obtención de información o evidencias, se puede realizar combinando uno o más de los siguientes procedimientos:

- Indagar y confirmar
- Inspeccionar

- Observar
- Recalcular y analizar
- Recolectar y analizar evidencia automatizada

3.2.2.5. Productos a Entregar

En base a la revisión llevada a cabo, se identificarán las debilidades de control en el Departamento de Recursos Informáticos, se elaborará un informe preliminar, el cual será presentado a la Jefatura del Departamento y a la Gerencia General, para posteriormente emitir un informe final, el cual será presentado a la Gerencia General de la empresa.

Las recomendaciones emitidas en base a las debilidades identificadas dependiendo de la factibilidad y posibilidad de la empresa, deberán ser implementadas en un lapso no superior a cinco meses y una vez que se haya realizado las correcciones en el departamento de Recursos Informáticos, este deberá ser evaluado.

3.2.2.6. Herramientas a Utilizar

La auditoría informática, se basa en una serie de análisis que se realiza con tres métodos base escogidos para la realización de este trabajo:

- Encuestas de evaluación acerca del uso de la tecnología
- Simulaciones de los procesos y casos
- Aplicación de escenarios tecnológicos

Además existen otros métodos, como son:

- Matrices de Investigación de Campo

Instrumento elaborado para ser utilizado como base de datos para la organización del trabajo del Equipo de Auditoría Informática de la ESPE.

- Observación Directa

Es una técnica que nos permite captar con todos nuestro sentido la realidad de la organización y puede ser de dos tipos. No participante, es aquella en que el auditor observa externamente el proceso sin interferir en ellos y, participante, es aquella en la que el auditor participa en los procesos de la unidad auditada, integrándose en el grupo y sus actividades. En cualquier caso, hay que definir el objetivo de la observación (cuál es el motivo de su realización), las variables de la observación (que queremos observar, planificación de la observación (que haremos durante la observación y transcripción de la observación (como se expresara la observación, por escrito, visualmente, etc.).

- Entrevistas

Es una técnica útil y arriesgada, ésta representa la inversión del territorio laboral de una persona, es lógico por lo tanto reacciones defensivas e incluso hostiles. Una forma de 'rebajar' la tensión, está en adoptar una postura amigable y de colaboración. El éxito de la entrevista, depende de los siguientes factores (repartidos por igual entre el auditor y el entrevistado): la experiencia y los conocimientos del auditor y la predisposición y los conocimientos del entrevistado.

- Checklist

El checklist es una técnica muy utilizada en el campo de la auditoría informática. No es más que una lista de comprobación o cuestionario, que sigue pautas determinadas, dependiendo de qué estemos evaluando o qué objetivos se desean alcanzar.

3.3. INVESTIGACIÓN DE CAMPO

3.3.1. Identificación de Riesgos de TI Críticos.

La matriz con la que se manejó los Riesgos de TI críticos, es la que se muestra a continuación, ésta corresponde correspondiente a los procesos críticos que se han encontrado en el sistema de la Cooperativa de Ahorro y Crédito “Alianza del Valle” Ltda. (La cual fue contestada por el responsable del sistema).

Tabla 2: Matriz de riesgos

| | | | Dominio General a analizar | | | | | | | |
|----------------|-----------------|---------------|--------------------------------------|-----------------------------------|---|--------|-------|------|--------------------|----------------|
| | | | Subdominio a analizar | | | | | | | |
| | | | Dominio General no requiere análisis | | | | | | | |
| Importancia | | | Proceso de TI | | | Riesgo | | | Control de Fuentes | |
| Muy importante | Algo importante | No importante | | | | Alto | Medio | bajo | Documentado | No Documentado |
| X | | | PO1 | Definir un Plan Estratégico de TI | x | | | X | | |
| | | | PO1.1 | Administración del valor de TI | | o | | | | |
| | | | PO1.2 | Alineación de Ti con el negocio | o | | | | | |
| | | | PO1.3 | Evaluación del desempeño actual | | o | | | | |

| | | | | | | | |
|---|--|--------|---|---|---|---|---|
| | | PO1.4 | Plan estratégico de TI | | o | | |
| | | PO1.5 | Planes tácticos de TI | | o | | |
| | | PO1.6 | Administración del portafolio de TI | | o | | |
| X | | PO2 | Definir la arquitectura de información | x | | | X |
| | | PO2.1 | Modelo de arquitectura de información empresarial | | o | | |
| | | PO2.2 | Diccionario de datos empresarial y reglas de sintaxis de datos | | o | | |
| | | PO2.3 | Esquema de clasificación de datos | o | | | |
| | | PO2.4 | Administración de la integridad | | | o | |
| X | | PO3 | Determinar la dirección tecnológica | | x | | X |
| | | PO3.1 | Planeación de la dirección tecnológica | | o | | |
| | | PO3.2 | Plan de infraestructura tecnológica | | | o | |
| | | PO3.3 | Monitoreo de tendencias y regulaciones futuras | | o | | |
| | | PO3.4 | Estándares tecnológicos | | o | | |
| | | PO3.5 | Consejo de arquitectura | | | o | |
| X | | PO4 | Definir los procesos, organización y relaciones de TI | | x | | X |
| | | PO4.1 | Marco de trabajo del proceso | | | o | |
| | | PO4.2 | Comité estratégico | | | o | |
| | | PO4.3 | Comité directivo | | | o | |
| | | PO4.4 | Ubicación organizacional de la función de TI | | | o | |
| | | PO4.5 | Estructura organizacional | | | o | |
| | | PO4.6 | Roles y responsabilidades | o | | | |
| | | PO4.7 | Responsabilidad de aseguramiento de calidad de TI | | | o | |
| | | PO4.8 | Responsabilidad sobre el riesgo, la seguridad y el cumplimiento | | | o | |
| | | PO4.9 | Propiedad de datos y de sistemas | | | O | |
| | | PO4.10 | Supervisión | | | o | |
| | | PO4.11 | Segregación de funciones | | | o | |
| | | PO4.12 | Personal de TI | | | o | |
| | | PO4.13 | Personal clave de TI | | | o | |
| | | PO4.14 | Políticas y procedimientos para personal contratado | | | O | |
| | | PO4.15 | Relaciones | | | o | |

| | | | | | | | | | |
|---|---|--|-------|---|---|---|---|---|--|
| | X | | PO5 | Administrar la inversión en TI | | X | | X | |
| | | | PO5.1 | Marco de trabajo para la administración financiera | | O | | | |
| | | | PO5.2 | Prioridades dentro del presupuesto de TI | | O | | | |
| | | | PO5.3 | Proceso presupuestal | | | o | | |
| | | | PO5.4 | Administración de costos | | | o | | |
| | | | PO5.5 | Administración de beneficios | | | o | | |
| X | | | PO6 | Comunicar las aspiraciones y la dirección de la gerencia | | X | | X | |
| | | | PO6.1 | Ambiente de políticas y de control | | O | | | |
| | | | PO6.2 | Riesgo corporativo y marco de referencia de control interno de TI | o | | | | |
| | | | PO6.3 | Administración de políticas para TI | | O | | | |
| | | | PO6.4 | Implantación de políticas de TI | | O | | | |
| | | | PO6.5 | Comunicación de los objetivos y la dirección de TI | | | o | | |
| X | | | PO7 | Administrar los recursos humanos de TI | | | x | X | |
| | | | PO7.1 | Reclutamiento y retención del personal | | O | | | |
| | | | PO7.2 | Competencias del personal | | | o | | |
| | | | PO7.3 | Asignación de roles | | | o | | |
| | | | PO7.4 | Entrenamiento del personal de TI | | | o | | |
| | | | PO7.5 | Dependencia sobre los individuos | | | o | | |
| | | | PO7.6 | Procedimientos de Investigación del personal | | | o | | |
| | | | PO7.7 | Evaluación del desempeño del empleado | | O | | | |
| | | | PO7.8 | Cambios y terminación de trabajo | | O | | | |
| X | | | PO8 | Administrar calidad | x | | | X | |
| | | | PO8.1 | Sistema de administración de calidad | | O | | | |
| | | | PO8.2 | Estándares y prácticas de calidad | o | | | | |
| | | | PO8.3 | Estándares de desarrollo y de adquisición | | O | | | |
| | | | PO8.4 | Enfoque en el cliente | | O | | | |
| | | | PO8.5 | Mejora continua | | O | | | |
| | | | PO8.6 | Medición, monitoreo y revisión de la calidad | o | | | | |
| X | | | PO9 | Evaluar y administrar los riesgos de TI | x | | | X | |

| | | | | | | | |
|---|--|---------|---|---|---|---|---|
| | | PO9.1 | Alineación de la administración de riesgos de TI y del negocio | o | | | |
| | | PO9.2 | Establecimiento del contexto del riesgo | | o | | |
| | | PO9.3 | Identificación de eventos | | o | | |
| | | PO9.4 | Evaluación de riesgos | | | o | |
| | | PO9.5 | Respuesta a los riesgos | | o | | |
| | | PO9.6 | Mantenimiento y monitoreo de un plan de acción de riesgos | | o | | |
| X | | PO10 | Administrar proyectos | | x | | X |
| | | PO10.1 | Marco de trabajo para la administración de programas | | | o | |
| | | PO10.2 | Marco de trabajo para la administración de proyectos | | | o | |
| | | PO10.3 | Enfoque de administración de proyectos | | o | | |
| | | PO10.4 | Compromiso de los interesados | | | o | |
| | | PO10.5 | Estatuto de alcance del proyecto | | o | | |
| | | PO10.6 | Inicio de las fases del proyecto | | o | | |
| | | PO10.7 | Plan integrado del proyecto | | o | | |
| | | PO10.8 | Recursos del proyecto | | | o | |
| | | PO10.9 | Administración de riesgos del proyecto | | | o | |
| | | PO10.10 | Plan de calidad del proyecto | | | o | |
| | | PO10.11 | Control de cambios del proyecto | | o | | |
| | | PO10.12 | Planeación del proyecto y métodos de aseguramiento | | o | | |
| | | PO10.13 | Medición del desempeño, reportes y monitoreo del proyecto | | o | | |
| | | PO10.14 | Cierre del proyecto | | | o | |
| X | | AI1 | Identificar soluciones automatizadas | | x | | X |
| | | AI1.1 | Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio | | | o | |
| | | AI1.2 | Reporte de análisis de riesgos | | o | | |
| | | AI1.3 | Estudio de factibilidad y formulación de cursos de acción alternativos | | o | | |
| | | AI1.4 | Requerimientos, decisión de factibilidad y aprobación | | | o | |
| X | | AI2 | Adquirir y mantener software aplicativo | | x | | X |
| | | AI2.1 | Diseño de alto nivel | | o | | |

| | | | | | | | |
|---|--|--------|--|---|---|---|---|
| | | AI2.2 | Diseño detallado | | o | | |
| | | AI2.3 | Control y adaptabilidad de las aplicaciones | | O | | |
| | | AI2.4 | Seguridad y disponibilidad de las aplicaciones | | O | | |
| | | AI2.5 | Configuración e implantación de software aplicativo adquirido | | O | | |
| | | AI2.6 | Actualizaciones importantes en sistemas existentes | | | o | |
| | | AI2.7 | Desarrollo de software aplicativo | | | o | |
| | | AI2.8 | Aseguramiento de la calidad del software | | | o | |
| | | AI2.9 | Administración de los requerimientos de aplicaciones | | | o | |
| | | AI2.10 | Mantenimiento de software aplicativo | | | o | |
| X | | AI3 | Adquirir y mantener infraestructura tecnológica | x | | | X |
| | | AI3.1 | Plan de adquisición de infraestructura tecnológica | o | | | |
| | | AI3.2 | Protección y disponibilidad del recurso de infraestructura | | O | | |
| | | AI3.3 | Mantenimiento de la infraestructura | o | | | |
| | | AI3.4 | Ambiente de prueba de factibilidad | | O | | |
| X | | AI4 | Facilitar la operación y el uso | | X | | X |
| | | AI4.1 | Plan para soluciones de operación | | O | | |
| | | AI4.2 | Transferencia de conocimiento a la gerencia del negocio | | O | | |
| | | AI4.3 | Transferencia de conocimiento a usuarios finales | | | o | |
| | | AI4.4 | Transferencia de conocimiento al personal de operaciones y soporte | | | o | |
| X | | AI5 | Adquirir recursos de TI | | X | | X |
| | | AI5.1 | Control de adquisición | | O | | |
| | | AI5.2 | Administración de contratos con proveedores | | | o | |
| | | AI5.3 | Selección de proveedores | | | o | |
| | | AI5.4 | Adquisición de software | | O | | |
| | | AI5.5 | Adquisición de recursos de desarrollo | | O | | |
| | | AI5.6 | Adquisición de infraestructura, | | | o | |

| | | | | | | | | |
|---|--|--------|--|---|---|---|---|---|
| | | | instalaciones y servicios relacionados | | | | | |
| X | | AI6 | Administrar cambios | x | | | X | |
| | | AI6.1 | Estándares y procedimientos para cambios | o | | | | |
| | | AI6.2 | Evaluación de impacto, priorización y autorización | | O | | | |
| | | AI6.3 | Cambios de emergencia | o | | | | |
| | | AI6.4 | Seguimiento y reporte del estatus de cambio | | o | | | |
| | | AI6.5 | Cierre y documentación del cambio | | o | | | |
| X | | AI7 | Instalar y acreditar soluciones y cambios | | x | | X | |
| | | AI7.1 | Entrenamiento | | | o | | |
| | | AI7.2 | Plan de prueba | | | o | | |
| | | AI7.3 | Plan de implementación | | | o | | |
| | | AI7.4 | Ambiente de prueba | | | o | | |
| | | AI7.5 | Conversión de sistema y datos | | o | | | |
| | | AI7.6 | Prueba de cambios | | o | | | |
| | | AI7.7 | Prueba final de aceptación | | o | | | |
| | | AI7.8 | Transferencia a producción | | | o | | |
| | | AI7.9 | Liberación de software | | | o | | |
| | | AI7.10 | Distribución del sistema | | | o | | |
| | | AI7.11 | Registro y rastreo de cambios | | o | | | |
| | | AI7.12 | Revisión posterior a la implantación | | o | | | |
| X | | DS1 | Definir y administrar los niveles de servicio | x | | | | X |
| | | DS1.1 | Marco de trabajo de la administración de los niveles de servicio | | o | | | |
| | | DS1.2 | Definición de servicios | | o | | | |
| | | DS1.3 | Acuerdos de niveles de servicio | | | o | | |
| | | DS1.4 | Acuerdos de niveles de operación | | o | | | |
| | | DS1.5 | Monitoreo y reporte del cumplimiento de los niveles de servicio | o | | | | |
| | | DS1.6 | Revisión de los acuerdos de niveles de servicio y de los contratos | | o | | | |
| X | | DS2 | Administrar los servicios de terceros | | x | | X | |
| | | DS2.1 | Identificación de las relaciones con todos los proveedores | | o | | | |

| | | | | | | | | |
|---|--|--------|--|---|---|---|---|--|
| | | DS2.2 | Administración de las relaciones con los proveedores | | | o | | |
| | | DS2.3 | Administración de riesgos del proveedor | | o | | | |
| | | DS2.4 | Monitoreo del desempeño del proveedor | | o | | | |
| X | | DS3 | Administrar el desempeño y la capacidad | x | | | X | |
| | | DS3.1 | Planeación del desempeño y la capacidad | | o | | | |
| | | DS3.2 | Capacidad y desempeño actual | o | | | | |
| | | DS3.3 | Capacidad y desempeño futuro | | | o | | |
| | | DS3.4 | Disponibilidad de recursos de TI | | o | | | |
| | | DS3.5 | Monitoreo y reporte | | o | | | |
| X | | DS4 | Garantizar la continuidad de los servicios | x | | | X | |
| | | DS4.1 | Marco de trabajo de continuidad | | O | | | |
| | | DS4.2 | Planes de continuidad de TI | o | | | | |
| | | DS4.3 | Recursos críticos de TI | | | o | | |
| | | DS4.4 | Mantenimiento del plan de continuidad de TI | | O | | | |
| | | DS4.5 | Pruebas del plan de continuidad de TI | | O | | | |
| | | DS4.6 | Entrenamiento del plan de continuidad de TI | | o | | | |
| | | DS4.7 | Distribución del plan de continuidad de TI | | o | | | |
| | | DS4.8 | Recuperación y reanudación de los servicios de Ti | | | o | | |
| | | DS4.9 | Almacenamiento de respaldos fuera de las instalaciones | | | o | | |
| | | DS4.10 | Revisión port-reanudacion | | o | | | |
| X | | DS5 | Garantizar la seguridad de los sistemas | x | | | X | |
| | | DS5.1 | Administración de la seguridad de TI | | o | | | |
| | | DS5.2 | Plan de seguridad de TI | | o | | | |
| | | DS5.3 | Administración de identidad | | | o | | |
| | | DS5.4 | Administración de cuentas del usuario | | o | | | |
| | | DS5.5 | Pruebas, vigilancia y monitoreo de la seguridad | | o | | | |
| | | DS5.6 | Definición de incidente de seguridad | | o | | | |
| | | DS5.7 | Protección de la tecnología de | | o | | | |

| | | | | | | | | |
|---|--|--------|---|---|---|---|--|--|
| | | | seguridad | | | | | |
| | | DS5.8 | Administración de llaves criptográficas | | o | | | |
| | | DS5.9 | Prevención, detección y corrección de software malicioso | | o | | | |
| | | DS5.10 | Seguridad de la red | o | | | | |
| | | DS5.11 | Intercambio de datos sensitivos | | o | | | |
| X | | DS6 | Identificar y asignar costos | x | | X | | |
| | | DS6.1 | Definición de servicios | | o | | | |
| | | DS6.2 | Contabilización de TI | | | o | | |
| | | DS6.3 | Modelación de costos y cargos | | | o | | |
| | | DS6.4 | Mantenimiento del modelo de costos | | | o | | |
| X | | DS7 | Educar y entrenar a los usuarios | x | | X | | |
| | | DS7.1 | Identificación de necesidades de entrenamiento y educación | | o | | | |
| | | DS7.2 | Impartición de entrenamiento y educación | | o | | | |
| | | DS7.3 | Evaluación del entrenamiento recibido | | | o | | |
| X | | DS8 | Administrar la mesa de servicio y los incidentes | x | | X | | |
| | | DS8.1 | Mesa de servicios | | | o | | |
| | | DS8.2 | Registro de consultas de clientes | | o | | | |
| | | DS8.3 | Escalamiento de incidentes | | o | | | |
| | | DS8.4 | Cierre de incidentes | | o | | | |
| | | DS8.5 | Análisis de tendencias | | o | | | |
| X | | DS9 | Administrar la configuración | x | | X | | |
| | | DS9.1 | Repositorio de configuración y línea base | | | o | | |
| | | DS9.2 | Identificación y mantenimiento de elementos de configuración | | o | | | |
| | | DS9.3 | Revisión de integridad de la configuración | | o | | | |
| X | | DS10 | Administración de problemas | x | | X | | |
| | | DS10.1 | Identificación y clasificación de problemas | | o | | | |
| | | DS10.2 | Rastreo y resolución de problemas | | o | | | |
| | | DS10.3 | Cierre de problemas | | o | | | |
| | | DS10.4 | Integración de las administración de cambios, configuración y problemas | | o | | | |

| | | | | | | | | |
|---|--|--------|---|---|---|---|---|--|
| X | | DS11 | Administración de la información | | x | | X | |
| | | DS11.1 | Requerimientos del negocio para administración de datos | | o | | | |
| | | DS11.2 | Acuerdos de almacenamiento y conservación | | | o | | |
| | | DS11.3 | Sistema de administración de librerías de medios | | o | | | |
| | | DS11.4 | Eliminación | | | o | | |
| | | DS11.5 | Respaldo y restauración | | | o | | |
| | | DS11.6 | Requerimientos de seguridad para la administración de datos | | o | | | |
| X | | DS12 | Administración del ambiente físico | x | | | X | |
| | | DS12.1 | Selección y diseño de datos | | o | | | |
| | | DS12.2 | Medidas de seguridad física | o | | | | |
| | | DS12.3 | Acceso Físico | o | | | | |
| | | DS12.4 | Protección contra factores ambientales | | o | | | |
| | | DS12.5 | Administración de instalaciones físicas | | o | | | |
| X | | DS13 | Administración de operaciones | | x | | X | |
| | | DS13.1 | Procedimientos e instrucciones de operaciones | | o | | | |
| | | DS13.2 | Programación de tareas | | | o | | |
| | | DS13.3 | Monitoreo de la infraestructura de TI | | o | | | |
| | | DS13.4 | Documentos sensitivos y dispositivos de salida | | o | | | |
| | | DS13.5 | Mantenimiento preventivo del hardware | | | o | | |
| X | | ME1 | Monitorear y evaluar el desempeño de TI | x | | | X | |
| | | ME1.1 | Enfoque del monitoreo | | o | | | |
| | | ME1.2 | Definición y recolección de datos de monitoreo | | | o | | |
| | | ME1.3 | Método de monitoreo | | o | | | |
| | | ME1.4 | Evaluación del desempeño | | | o | | |
| | | ME1.5 | Reportes al consejo directivo y a ejecutivos | | o | | | |
| | | ME1.6 | Acciones correctivas | | o | | | |
| X | | ME2 | Monitorear y evaluar el control interno | x | | | X | |
| | | ME2.1 | Monitorear el marco de trabajo de control interno | | o | | | |

| | | | | | | | | |
|---|--|-------|---|---|---|---|--|--|
| | | ME2.2 | Revisiones de auditoría | o | | | | |
| | | ME2.3 | Excepciones de control | | o | | | |
| | | ME2.4 | Auto-evaluación de control | | o | | | |
| | | ME2.5 | Aseguramiento del control interno | o | | | | |
| | | ME2.6 | Control interno para terceros | | o | | | |
| | | ME2.7 | Acciones correctivas | o | | | | |
| X | | ME3 | Garantizar el cumplimiento regulatorio | | x | | | |
| | | ME3.1 | Identificar las leyes y regulaciones con impacto potencial sobre TI | | o | | | |
| | | ME3.2 | Optimizar la respuesta a requerimientos regulatorios | | o | | | |
| | | ME3.3 | Evaluación del cumplimiento con requerimientos regulatorios | | o | | | |
| | | ME3.4 | Aseguramiento positivo del cumplimiento | | o | | | |
| | | ME3.5 | Reportes integrados | | | o | | |
| X | | ME4 | Proporcionar gobierno de TI | x | | | | |
| | | ME4.1 | Establecer un marco de trabajo de gobierno para TI | | o | | | |
| | | ME4.2 | Alineamiento estratégico | | o | | | |
| | | ME4.3 | Entrega de valor | | o | | | |
| | | ME4.4 | Administración de recursos | | | o | | |
| | | ME4.5 | Administración de riesgos | | | o | | |
| | | ME4.6 | Medición del desempeño | | o | | | |

3.3.2. Matriz de Investigación de Campo

Tabla 3: Matriz de investigación de campo

| OBJETIVOS DE CONTROL DETALLADOS | | CONTROLES POR VERIFICAR | Prueba del Control | DOCUMENTACIÓN DE REFERENCIA | PREGUNTAS BASICAS | INSTRUMENTOS DE INVESTIGACION DE CAMPO |
|---------------------------------------|--|---|---|---|---|--|
| Nombre | Descripción | | | | | |
| PO1.2 Alineación de TI con el negocio | Educar a los ejecutivos sobre las capacidades tecnológicas actuales y sobre el rumbo futuro, sobre las oportunidades que ofrece TI y, sobre qué debe hacer el negocio para capitalizar esas oportunidades. Asegurarse de que el rumbo del negocio al cual está alineado la TI está bien entendido. Las estrategias de negocio y de TI deben estar integradas, relacionando de manera | 1) Plan de capacitación al usuario sobre tecnologías de TI 2) Plan estratégico TI alineado con plan estratégico de negocio | 1) <u>Anexo A.1:</u> <u>Hoja de Evaluación</u> <u>PO1</u> | Plan de capacitaciones. Plan estratégico de negocio. Plan de TI | 1) Cada proyecto cuenta con una justificación relacionada con el plan estratégico y operativo de negocios de la empresa? 2) Conoce la importancia de TI para el negocio y su crecimiento? 3) A futuro TI garantiza una mejor capitalización del negocio ? | Cuestionario y entrevista. |

| | | | | | | |
|---|---|---|---|---|--|-----------------------------------|
| | <p>clara las metas de la empresa y las metas de TI y reconociendo las oportunidades así como las limitaciones en la capacidad actual y, se deben comunicar de manera amplia.</p> <p>Identificar las áreas en que el negocio (estrategia) depende de forma crítica de la TI y, mediar entre los imperativos del negocio y la tecnología, de tal modo que se puedan establecer prioridades concertadas.</p> | | | | | |
| PO2.3 Esquema de clasificación de datos | <p>Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información (esto es, pública, confidencial, secreta) de la empresa. Este esquema incluye detalles acerca de la</p> | <p>1) Esquema de clasificación de datos</p> <p>2) Requerimientos de manejo de datos</p> <p>3) Descripción de permisos de usuario para control de acceso</p> | <p>1) <u>Anexo A.2:</u></p> <p><u>Hoja de Evaluación</u></p> <p><u>PO2</u></p> | <p>Manual general de políticas de gestión de informática y tecnología</p> | <p>1) La información que el negocio genera, es tratada con la confidencialidad que requiere el caso?</p> <p>2) Es el personal consiente del perfil que maneja cuando genera o extrae información del sistema? 3)</p> | <p>Cuestionario y entrevista.</p> |

| | | | | | | |
|---|--|--|---|---|---|-----------------------------------|
| | <p>propiedad de datos, la definición de niveles apropiados de seguridad y de controles de protección y, una breve descripción de los requerimientos de retención y destrucción de datos, además de qué tan críticos y sensibles son. Se usa como base para aplicar controles como el control de acceso, archivo o inscripción.</p> | | | | <p>El modelo de datos es fácil de utilizar ?</p> | |
| <p>PO9.1 Alineación de la administración de riesgos de TI y del negocio</p> | <p>Integrar el gobierno, la administración de riesgos y el marco de control de TI, al marco de trabajo de administración de riesgos de la organización. Esto incluye la alineación con el apetito de riesgo y con el nivel de tolerancia al riesgo de la organización</p> | <p>1) Marco de administración de riesgos de TI 2) Marco de trabajo de administración de riesgos del negocio.</p> | <p>1) <u>Anexo A.3:</u> <u>Hoja de Evaluación</u> <u>PO9</u></p> | <p>se solicita a la Cooperativa un marco de administración de riesgos de TI y el marco de trabajo de administración de riesgos de negocio</p> | <p>1) Existen reportes de monitoreo de riesgos activados? 2) Los planes de administración de riesgos son aprobados por la gerencia?</p> | <p>Cuestionario y entrevista.</p> |

| | | | | | | |
|---|--|---|---|--|---|-----------------------------------|
| <p>AI3.1 Plan de adquisición de infraestructura tecnológica</p> | <p>Generar un plan para adquirir, implantar y mantener la infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio y, que esté de acuerdo con la dirección tecnológica de la organización. El plan debe considerar extensiones futuras para adiciones de capacidad, costos de transición, riesgos tecnológicos y vida útil de la inversión para actualizaciones de tecnología. Evaluar los costos de complejidad y la viabilidad comercial del proveedor y el producto al añadir nueva capacidad técnica</p> | <p>1) Plan de adquisición implantación y mantenimiento de infraestructura tecnológica. 2) Planificación de TI</p> | <p>1) Anexo A.4: Hoja de Evaluación AI3</p> | <p>Solicitar a la Cooperativa el plan de adquisición, implantación y mantenimiento de la infraestructura tecnológica Plan de Administración de cambios</p> | <p>1) Cuantos proyectos están sujetos a factibilidad dentro del plan anual de los TI? 2) Cuantos proyectos de TI han sido entregados a tiempo según el presupuesto y planificación?</p> | <p>Cuestionario y entrevista.</p> |
|---|--|---|---|--|---|-----------------------------------|

| | | | | | | |
|---|--|--|--|--|---|--|
| <p>AI3.3 Mantenimiento de la Infraestructura</p> | <p>Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo con el procedimiento de administración de cambios de la organización. Incluir una revisión periódica contra las necesidades del negocio, administración de parches y estrategias de actualización, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.</p> | <p>1) Plan de manteamientos de infraestructura tecnológica 2) Plan de administración de cambios infraestructura tecnológica</p> | | | <p>1) En qué porcentaje los usuarios se sienten satisfechos con la funcionalidad y mantenimiento de TI? 2) Con qué frecuencia con la que se realiza un mantenimiento? 3) Que procedimiento realiza para poder recibir un mantenimiento correctivo o preventivo ?</p> | |
|---|--|--|--|--|---|--|

| | | | | | | |
|---|--|--|---|---|---|-----------------------------------|
| <p>AI6.1 Estándares y procedimientos para cambios</p> | <p>Establecer procedimientos de administración de cambio formales para manejar de manera estándar todas las solicitudes (incluyendo mantenimiento y parches) para cambios a aplicaciones, procedimientos, procesos, parámetros de sistema y servicio y, las plataformas fundamentales.</p> | <p>1) Manual de gestión y desarrollo de software</p> | <p>1) <u>Anexo A.5:</u> <u>Hoja de Evaluación AI6</u></p> | <p>Solicitar a la Cooperativa el manual de gestión y desarrollo de software</p> | <p>1) Procedimiento que necesario para realizar un cambio o mantenimiento de software? 2) Como se controla el acceso a los programas fuentes?</p> | <p>Cuestionario y entrevista.</p> |
| <p>AI6.3 Cambios de emergencia</p> | <p>Establecer un proceso para definir, plantear, evaluar y autorizar los cambios de emergencia que no sigan el proceso de cambio establecido. La documentación y pruebas se realizan, posiblemente, después de la implantación del cambio de emergencia.</p> | <p>1) Manual de gestión y desarrollo de software</p> | <p>1) <u>Anexo A.5:</u> <u>Hoja de Evaluación AI6</u></p> | | <p>1) Número de interrupciones o errores reportados y solucionados emergentemente? 2) Que cambios se han realizado emergentemente a la infraestructura? 3) Cual es el procedimiento para cambios emergentes ?</p> | |

| | | | | | | |
|---|--|---|--|---|--|----------------------------|
| DS1.5 Monitoreo y reporte del cumplimiento de los niveles de servicio | Monitorear continuamente los criterios de desempeño especificados para el nivel de servicio. Los reportes sobre el cumplimiento de los niveles de servicio deben emitirse en un formato que sea entendible para los interesados. Las estadísticas de monitoreo son analizadas para identificar tendencias positivas y negativas tanto de servicios individuales como de los servicios en conjunto. | 1) Marco de administración de niveles de servicio 2) Reportes de cumplimiento de niveles de servicio. | 1) <u>Anexo A.6:</u> <u>Hoja de Evaluación</u> <u>DS1</u> | Solicitar como se procede en la administración de niveles de servicio del departamento de tecnología y sistemas | 1) Que servicios han sido entregados y no se encuentran en el catalogo? 2) Que niveles de servicio son medidos por el departamento de TI ? 3) Que porcentaje de usuarios se encuentran satisfechos con los niveles de servicio que brinda la empresa? | Cuestionario y entrevista. |
| DS3.2 Capacidad y desempeño actual | Revisar la capacidad y desempeño actual de los recursos de TI en intervalos regulares para determinar si existe suficiente capacidad y desempeño para prestar los servicios con base en los niveles de servicio acordados. | 1) Manual técnico del sistema COBIS 2) Manual técnico de la base de datos 3) Esquema de distribución de red | 1) <u>Anexo A.7:</u> <u>Hoja de Evaluación</u> <u>DS3</u> | Solicitar a la Cooperativa toda la información acerca del Core Bancario COBIS, manual técnico de la base de datos y esquema de distribución de red. | 1) Cuantos son los activos que intervienen en el buen funcionamiento de este sistema? 2) Seguridades de la base de datos y tablas de auditoría del sistema COBIS? 3) Los tiempos de | Cuestionario y entrevista. |

| | | | | | | |
|-----------------------------------|---|--|--|----------------------------|---|----------------------------|
| | | | | | ejecución en las transacciones son los adecuados aspirados ? | |
| DS4.2 Planes de continuidad de TI | Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio. Los planes deben considerar requerimientos de resistencia, procesamiento alternativo y, capacidad de recuperación de todos los servicios críticos de TI. También deben cubrir los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas | 1) Plan de contingencia de TI 2) Requerimientos de los servicios críticos de TI | 1) <u>Anexo A.8:</u> <u>Hoja de Evaluación</u> <u>DS4</u> | Plan de contingencia de TI | 1) Que tiempo transcurre entre las pruebas de cualquier elemento dado del plan de continuidad? 2) Con qué frecuencia existen interrupciones ? | Cuestionario y entrevista. |

| | | | | | | |
|---------------------------------------|---|---|---|--|--|-----------------------------------|
| <p>DS5.10 Seguridad de la red</p> | <p>Garantizar que se utilizan técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes y, detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.</p> | <p>1) Políticas internas de seguridad en la red</p> | <p>1) <u>Anexo A.9:</u> <u>Hoja de Evaluación</u> <u>DS5</u></p> | <p>Políticas internas de seguridades de la red</p> | <p>1) Número de incidentes con impacto negativo al negocio 2) Tiempos para otorgar, cambiar o eliminar privilegios de acceso</p> | <p>Cuestionario y entrevista.</p> |
|---------------------------------------|---|---|---|--|--|-----------------------------------|

| | | | | | | |
|---|---|--|--|---|---|-----------------------------------|
| <p>DS12.2 Medidas de seguridad física</p> | <p>Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio. Las medidas deben incluir, pero no limitarse al esquema del perímetro de seguridad, de las zonas de seguridad, la ubicación de equipo crítico y de las áreas de envío y recepción. En particular, mantenga un perfil bajo respecto a la presencia de operaciones críticas de TI. Deben establecerse las responsabilidades sobre el monitoreo y los procedimientos de reporte y de resolución de incidentes de seguridad física.</p> | <p>1) Regulamiento estándar de seguridades físicas</p> | <p>1) <u>Anexo A.10:</u> <u>Hoja de Evaluación</u> <u>DS12</u></p> | <p>Regulamiento estándar de seguridades físicas</p> | <p>1) Frecuencia de capacitación del personal respecto a medidas de protección, de seguridad y de instalaciones. 2) Cantidad de personal capacitado en medidas de protección, seguridad y de instalaciones.</p> | <p>Cuestionario y entrevista.</p> |
|---|---|--|--|---|---|-----------------------------------|

CAPÍTULO IV

Informe y resultados de la Investigación de Campo enfocándose a los 4 Dominios del Modelo COBIT 4.0

4.1.INTRODUCCIÓN

Luego de llevar a cabo la revisión de la documentación del Departamento de Sistemas, que es utilizado en la Cooperativa de Ahorro y Crédito “Alianza del Valle” Ltda.y, de ejecutar el análisis respectivo, de acuerdo a la Guía de Auditoría de COBIT, se pudieron obtener conclusiones que nos permitieron generar recomendaciones, mismas que se indican en el INFORME PRELIMINAR, el cual fue presentado y discutido con el encargado del Departamento de Sistemas, recibiendo del mismo las justificaciones respectivas, relacionadas con algunas observaciones, ante lo cual se creyó conveniente levantar la observación.

Posteriormente se elaboró el informe final de la auditoría, el cual ha sido enviado a la Gerencia (sección 4.4). El documento incluye un resumen gerencial (sección 4.2) junto con las conclusiones y recomendaciones realizadas.

4.2.RESUMEN EJECUTIVO

El objetivo principal de la auditoría, es detectar si la gestión del departamento de T.I. es adecuada para cubrir todas las necesidades del la Cooperativa de Ahorro y Crédito “Alianza del Valle”.

La auditoría se realizo en función de entrevistas y obtención de información, sostenidas con el personal del área de sistemas de la cooperativa, en donde efectuamos evaluaciones de las políticas, controles de aplicación y procedimientos de Ti existentes.

El contenido de esta auditoría está basado en 4 pilares de revisión que son:

- Evaluación Cobis
- Evaluación Base de Datos Sybase
- Evaluación Hardware y Software
- Evaluación Comunicaciones

Estos pilares se traducen en 10 procesos de evaluación Cobit que se detallan a continuación:

PLANEAR Y ORGANIZAR

PO1: Definir un Plan Estratégico de TI

PO2: Definir la arquitectura de la Información.

PO9: Evaluar y Administrar los Riesgos de TI

ADQUIRIR E IMPLEMENTAR

AI3: Adquirir y mantener infraestructura tecnológica

AI6: Administrar cambios

ENTREGAR Y DAR SOPORTE

DS1: Definir y Administrar los niveles de Servicio

DS3: Administrar el desempeño y la capacidad

DS4: Garantizar la continuidad del servicio

DS5: Garantizar la seguridad de los sistemas

DS12: Administrar el Ambiente Físico

Se inició la auditoría realizando la investigación de los procesos que se consideran prioritarios para la empresa, considerando su funcionamiento e importancia, además evaluando los posibles riesgos según los recientes eventos que hayan afectado al proceso.

A continuación se detalla el resumen ejecutivo presentado a la alta gerencia: **(VER ANEXO D)**

4.3. DESCRIPCIÓN DEL TRABAJO EFECTUADO

Una vez analizada y conocida de la situación actual de la entidad y, definido el enfoque de auditoría a ser utilizado, así como los responsables de la parte tecnológica y del negocio; en esta etapa se realizarán las siguientes actividades:

- Detallar la manera en que se probará cada una de las actividades de control, señaladas en el enfoque de auditoría, tanto en su implementación, como en su eficacia operativa.
- Determinar la documentación necesaria, para probar cada actividad de control identificada en el enfoque de auditoría (Anexo C).
- Planificar encuestas, Checklist, hojas de evaluación y entrevistas con los encargados del Área de Sistemas de la Cooperativa Alianza del Valle, con la finalidad de conocer más a detalle los procesos y procedimientos existentes en la entidad y solicitar la documentación identificada en el punto anterior.
- Una vez obtenida la información, realizar su respectivo análisis y documentación, en concordancia con el primer punto, esto con la finalidad de emitir una conclusión para cada actividad de control.
- Una vez analizados los atributos de control de cada actividad, emitir una conclusión acerca de la implementación y de la eficacia operativa de cada objetivo de control.
- Diseñar y elaborar el informe de auditoría, donde por cada Objetivo de Control se detallará:
 - Criterio
 - Condición

- Causa
 - Efecto
 - Conclusiones
 - Recomendaciones
-
- Verificar y discutir con la administración de la entidad, todas las oportunidades de mejora encontradas, con la finalidad de conocer su opinión al respecto.

 - Después de discutidas las conclusiones y recomendaciones, con la administración de la entidad, indicar en el informe su respuesta a cada una.

 - Emitir el informe final de auditoría, en el cual a más de lo indicado anteriormente, se adjuntará la respuesta de la administración para cada una de las recomendaciones emitidas.

4.4.RESULTADOS – INFORME DE LAS RECOMENDACIONES ACORDADAS CON LAS AUTORIDADES PERTINENTES

En conformidad con el Plan del proyecto de tesis, “**AUDITORÍA INFORMÁTICA DE LA COOPERATIVA DE AHORRO Y CREDITO “ALIANZA DEL VALLE” LTDA**”, se analizó cada uno de los controles referentes a los dominios en estudio, Planificación y Organización ,Adquisición e implementación, Soporte y servicios, Evaluación y seguimiento en la Cooperativa de Ahorro y Crédito “Alianza del Valle”, de la que se detallan a continuación las observaciones y recomendaciones resultantes de la revisión, en base a la aplicación del marco de referencia COBIT v. 4.0.

INFORME DETALLADO

ANTECEDENTES:

- La Cooperativa de Ahorro y Crédito “Alianza del Valle”, ha solicitado a través del departamento de auditoría interna y de la gerencia tecnológica. la ejecución de una auditoría informática, misma que se realizó desde el 1 de Agosto del 2011 al 14 de Diciembre del 2011.
- El Equipo de Auditoría, estuvo conformado por docentes y egresados de la Carrera de Ingeniería en Sistemas e Informática de la ESPE.
- En base a los lineamientos del Marco de Referencia de COBIT v. 4.0, se desarrolló el trabajo, para el efecto se cumplieron visitas a las agencias, se aplicaron encuestas y entrevistas al personal, se ejecutaron exámenes especiales a áreas críticas, como son :
Core Bancario Cobis, Base de Datos Sybase, Hardware y Comunicaciones.
- Cabe indicar que durante la evaluación, las debilidades detectadas, fueron puestas en conocimiento del Asistente de Gerencia y el Director de Informática y Comunicaciones, en reuniones de trabajo, a fin de que se tomen las medidas correctivas correspondientes con la agilidad del caso.

OBJETIVO:

Realizar una Auditoría Informática de los Sistemas de Información Tecnológicos de la Cooperativa de Ahorro y Crédito “Alianza del Valle LTDA.”, mediante la revisión del ambiente de control implementado en los procesos automatizados y en el gerenciamiento de los mismos, utilizando COBIT, a fin de identificar debilidades y emitir recomendaciones que permitan minimizar los riesgos.

GRUPO DE TRABAJO:

Ing. Mario Ron (Jefe de Proyecto)
Eco. Gabriel Chiriboga (Consultor)
Srta. Gabriela Barros
Srta. Andrea Cadena

PERSONAL DE LA DIRECCIÓN DE INFORMÁTICA Y

COMUNICACIONES:

Ing. Cesar Obando (Director de la DIC)
Tec. Jenny Gualotuña (Administrador de Ti)
Tec. Daniel Ortiz (Administrador del Centro de Cómputo)

PERIODO DE EJECUCION:

1 Agosto 2011 – 14 Diciembre 2011

MARCO DE REFERENCIA UTILIZADO

COBIT es un Marco de referencia de procesos y objetivos de control TI que pueden ser implementados para controlar, auditar y administrar la organización TI. Este Marco de referencia está basado en las mejores prácticas y sistemas de información de auditoría y control.

Esto en particular aspira a ayudar a los líderes empresariales a entender y administrar los riesgos relacionados con la tecnología de la Información y la relación entre los procesos de administración, las preguntas técnicas, la necesidad de controles y los riesgos.

COBIT está estructurado por 4 campos principales de administración, los cuales a su vez implican 34 procesos de administración asociados con la tecnología de la información. Cada proceso TI provee una descripción de

los requerimientos del negocio e identifica los asuntos claves que deben ser llevados a cabo para administrar exitosamente estos procesos.

Los recursos de TI y los criterios de la información requeridos para asegurar el éxito son también identificados para cada proceso TI. Para soportar una auto-evaluación, COBIT incluye un modelo de madurez para cada proceso TI. Estos modelos de madurez son similares en sus conceptos básicos utilizados por otros marcos referenciales, pero así como los 34 proceso TI de COBIT cubren todos los aspectos de TI, los modelos pueden ser utilizados para soportar la evaluación de toda la organización TI, en lugar de especializarse en determinadas áreas. Como soporte a la medición del rendimiento operacional, factores críticos de éxito, indicadores clave de logro de objetivos, e indicadores clave de rendimiento son identificados en cada proceso.

COBIT ofrece un conjunto de herramientas para administrar los procesos TI unificando los dos puntos de vista, el de la administración y el del auditor. Las Guías de Administración TI consideran los controles TI desde una perspectiva de la administración, mientras que las Guías de Auditoría proveen asistencia específica a los auditores en el diseño de programas adecuados de auditoría para cada dominio. COBIT también provee herramientas detalladas y personalizables de auto evaluación en forma de matrices y plantillas para asistir en la evaluación y medición de la organización comparada con los criterios de COBIT.

En resumen, COBIT, es una herramienta desarrollada para ayudar a los administradores de negocios a entender y administrar los riesgos asociados con la implementación de nuevas tecnologías y demostrar a las entidades reguladoras e inversionistas, que tan efectiva es su tarea.

Se ha definido a COBIT como: "Una estructura de relaciones y procesos para direccionar y controlar la compañía para lograr la consecución de los objetivos del negocio, entregando valor agregado mientras se administra el riesgo en función del ambiente de sistemas y sus procesos". Ver informe detallado (**Anexo E**).

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Al culminar el proyecto de la evaluación técnica e informática de los sistemas tecnológicos de información, de la Cooperativa de Ahorro y Crédito “Alianza del Valle” Ltda., se han cumplido con los objetivos propuestos en el presente trabajo, por lo tanto se exponen a continuación las siguientes conclusiones y recomendaciones en torno a la realización del proyecto.

- Para el desarrollo de una Auditoría Informática de los Sistemas de Información es de principal importancia contar con la guía de un marco de referencia. Para este proyecto se ha escogido el modelo COBIT desarrollado por ISACA, el cual a través de sus 4 dominios ofrece una serie de objetivos de control que permiten evaluar eficientemente el ambiente de control de una entidad, garantizando que TI está alineada con el negocio y que los riesgos de TI se administren apropiadamente.
- Al alinear la Normativa emitida por la Superintendencia de Bancos respecto a Tecnologías de la Información y los objetivos de control propuestos por COBIT se logró identificar y valorar los riesgos dentro de la entidad para tomar las medidas pertinentes y minimizar la materialización de los riesgos identificados.
- Durante el análisis y evaluación del ambiente de control en la entidad aplicando los dominios propuestos por COBIT se logró identificar debilidades obteniendo observaciones y recomendaciones para ser emitidas en el informe final, para llevar a cabo el proceso de la Auditoría es de suma importancia contar con el compromiso y apertura a la Auditoría Informática de los sistemas de información; de los principales involucrados como son las Autoridades superiores de la Cooperativa, el personal del departamento de sistemas y el Departamento de Auditoría Interna.

- La Auditoría de Ti en la Cooperativa propone mejoras a los controles existentes en la misma, pues sabiendo que si los controles facilitan la rendición de cuentas mediante la evidencia; al mejorar los controles que están fallando se logrará mitigar los riesgos. La Administración debe identificarse y conocer plenamente los controles.

- De acuerdo con lo planteado y el proyecto realizado es responsabilidad de la entidad aplicar y poner en marcha las recomendaciones emitidas de la Auditoría Informática, llevando a cabo esto de acuerdo a su capacidad y crecimiento.

- Luego de la revisión se analizo el nivel me madurez en que actualmente se encuentra la empresa según los riesgos y fallas encontradas y se determina el nivel al que se puede ascender si se cumplen con las recomendaciones planteadas. **(Ver Anexo F)**

ANEXOS

BIBLIOGRAFÍA:

- ISACA COBIT3 y COBIT 4
- Wikipedia
- <http://www.solomanuales.org/curso->
<http://www.monografias.com/trabajos5/audi/audi.shtml>
- <http://dmi.uib.es/~bbuades/auditoría/auditoría.PPT#266,11, Metodología>
(2)
- <http://www.audit.gov.tw/span/span2-2.htm>
- Auditoría Mario B. Ron Resumen
- Marco Conceptual Modelo COBIT / Mario B. Ron
- Fases de una Auditoría / Mario B. Ron
- “Evaluación de los Sistemas de Tecnología Informática y Revisión de las Seguridades de Plataforma Específica para la empresa EMAPA-I”/
Andrea M. Tobar.
- Management Guidelines – Cobit 3rd Edition, Objetivos de Control Cobit,
Resumen Ejecutivo Cobit, Marco Referencial Cobit, Implementation Tool
Set – Cobit 3rd Edition
- Modelo Coso Report
- Auditoría interna moderna de Brink y UIT
- WHITTINGTON, O. Ray, PANY Kurt, Auditoría: Un enfoque Integral,
Irwin McGrawHill, 12^a. Edición, Santa Fe de Bogota, Colombia, 2000
- Normas de Auditoría Interna emitidas por el The Institute of Internal
Auditors
- Enciclopedia de la Auditoría, Grupo Editorial Océano, Barcelona,
España, 1999
- ARENS, Alvin, Auditoría: Un enfoque integral, Prentice Hall
- Guía de Auditoría, McGrawHill, México, 1996
- Robert L. Grinaker Ben B. Barr, Auditoría Examen de los Estados
Financieros México 1989
- MEIGS, Principios de Auditoría, Editorial Diana México 1975
- Maldonado Milton, Auditoría de Gestión – Economía, Ecología, Eficacia,
Eficiencia, Ética, 2001
- Auditoría Operacional de José Dagoberto Pinilla

- <http://www.monografias.com/trabajos14/auditoriasistemas/auditoriasistemas.shtml>
- Auditoría Informática, Gonzalo Alonso Rivas, 1998 ediciones Díaz de Santos ISBN 84-87189-13.
- Auditoría en Informática Un enfoque metodológico y práctico, Lic. Enrique Hernández Hernández, 2002 editorial continental ISBN 970-24-0042-2.
- Auditoría informática, Echenique García José Antonio, segunda edición.
- Auditoría informática, Piattini Velthuis Mario Gerardo y Del Peso Navarro Emilio, segunda edición.
- COBIT versión 4
- http://www.network-sec.com/COBIT_DS
- <http://itil.osiatis.es/>
- <http://www.adacsi.org.ar/es/content.php>
- <http://www.reddeabastecimiento.org/COBIT%204.pdf>
- <http://www.auditoriasistemas.com/>
- <http://dmi.uib.es/~bbuades/auditoria/sld006.htm>
- <http://www.monografias.com/trabajos5/audi/audi.shtml>
- <http://www.audit.gov.tw/span/span2-2.htm>
- Auditoría Mario B. Ron Resumen
- Marco Conceptual Modelo COBIT / Mario B. Ron
- Fases de una Auditoría / Mario B. Ron
- “Evaluación de los Sistemas de Tecnología Informática y Revisión de las Seguridades de Plataforma Escuela Politécnica del Ejército para la empresa EMAPA-I”/ Andrea M. Tobar.
- Management Guidelines – Cobit 3rd Edition, Objetivos de Control Cobit, Resumen Ejecutivo Cobit, Marco Referencial Cobit, Implementation Tool Set – Cobit 3rd Edition
- Modelo Coso Report
- Auditoría interna moderna de Brink y UIT
- WHITTINGTON, O. Ray, PANY Kurt, Auditoría: Un enfoque Integral, Irwin McGrawHill, 12ª. Edición, Santa Fe de Bogota, Colombia, 2000
- Normas de Auditoría Interna emitidas por el The Institute of Internal Auditors

- Enciclopedia de la Auditoría, Grupo Editorial Océano, Barcelona, España, 1999
- ARENS, Alvin, Auditoría: Un enfoque integral, Prentice Hall
- Guía de Auditoría, McGrawHill, México, 1996
- Robert L. Grinaker Ben B. Barr, Auditoría Examen de los Estados Financieros México 1989
- MEIGS, Principios de Auditoría, Editorial Diana México 1975

HOJA DE LEGALIZACIÓN DE FIRMAS

ELABORADA POR

Gabriela Fernanda Barros Marcillo.

Andrea Erika Cadena Marten.

DIRECTOR DE LA CARRERA

Ing. Mauricio Campaña

Lugar y fecha: _____