# AUDITORÍA INFORMÁTICA DE LA COOPERATIVA DE AHORRO Y CRÉDITO ALIANZA DEL VALLE LTDA CON COBIT 4.0

*Andrea Cadena Marten, Gabriela Barros Marcillo, Ing. Mario Ron Egas, Eco. Gabriel Chiriboga*

1 Escuela Politécnica del Ejército, Quito Ecuador, lamartencita@hotmail.com

2 Escuela Politécnica del Ejército, Quito Ecuador, gabsbarros_88@yahoo.com

3 Politécnica del Ejército, Quito Ecuador, mbron@gmail.com

4 Politécnica del Ejército, Quito Ecuador, Gabriel_chiriboga@andinanet.net

**RESUMEN**

*El siguiente artículo presenta la Auditoria Informática de los Sistemas Tecnológicos de Información realizada a la Cooperativa de Ahorro y Crédito "Alianza del Valle". Ltda. Utilizando COBIT 4.0 que es un estándar internacional de buenas prácticas en administración y gobierno de tecnologías de información, que permite una alineación efectiva entre TI y los objetivos de negocio. El objeto de esta revisión técnica es identificar debilidades y emitir recomendaciones que permitan minimizar riesgos.*

*Para llevar a cabo este ejercicio de Auditoria, se elaboró una matriz de riesgos, para establecer los más críticos y enfocar la evaluación hacia ellos, con este resultado se elaboró un plan de investigación de campo o programa detallado de auditoría, en el que se establecen los diferentes instrumentos de evaluación y prueba de los controles. Luego de efectuar la investigación de campo se ordenó y analizó la información en forma comparativa, tomando como referencia los criterios de la norma antes indicada. Como resultado del análisis se elaboraron las observaciones y recomendaciones incluidas en dos informes: uno gerencial y otro detallado, los que conjuntamente con la carpeta de evidencias fue aceptado luego de las lecturas de estos informes en borrador y definitivo, el que contiene también los puntos de vista de los auditados.*

***Palabras Clave:*** Auditoria Informática, Ambiente de Control, Ti, Cobit 4.0, Cooperativa Alianza del Valle.

**ABSTRACT**

*This article aims to explain the process of achieving an Audit in the field of System Information for the Valley Alliance Mutual (Cooperativa de Ahorro y Crédito "Alianza del Valle" Ltda.). along with COBIT 4.0, a tool developed to help business managers understand and manage risks related to the implementation of new technologies. COBIT runs through the finest controlled environment that focuses on optimizing the value of IT thus achieving a successful design between IT and business goals. The sole purpose of this technical review is to identify weaknesses and build suggestions minimizing risks.*

*To carry out this audit it was necessary to send a list of requirements to the entity, conducting a comprehensive analysis of the documents submitted to the audit team in order clarify certain points of proposed questions from the documents thus developing surveys to the staff of the entity receiving a clear response. According to the results of these surveys, interviews will be conducted as an audit method to customize further investigation, based on these surveys and interviews we were able to unfold and collect substantial tests and evidence. Hence the results of the surveys, interviews and substantial testing and the alignment of the results to each objective proposed by COBIT, we were able to obtain the observations and suggestions to be issued as a statement to the management.*

***KeyWords:*** Computer-Audit, Environment-Control, Ti, Cobit, Cooperativa Alianza del Valle.

## 1. INTRODUCCIÓN

Los Sistemas Informáticos deben integrarse a la gestión empresarial; a través de normas y estándares informáticos implementados mediante controles en los procesos que cumplen los sistemas como apoyo al negocio, especialmente en la toma de decisiones.

En el desarrollo tecnológico que realiza la Cooperativa de Ahorro y Crédito Alianza del Valle, es necesario una Auditoria Informática, que permita asegurar que las soluciones propuestas e implantadas son las adecuadas para el correcto funcionamiento del negocio financiero en el que se desenvuelve la Cooperativa y que los riesgos han sido minimizados reduciéndolos al máximo posible en razón de su eficiencia y eficacia.

La evaluación de los sistemas informáticos, 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 sometida la Cooperativa Alianza del Valle y recomendar procedimientos que permitan minimizarlos o eliminarlos.

El análisis de los Objetivos de Control con COBIT debe ser de carácter objetivo e independiente, crítico, basado en evidencia, 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 eficiencia el uso de los recursos informáticos, validez de la información y efectividad de los controles establecidos.

El proyecto de plan de tesis “AUDITORÍA INFORMÁTICA DE LA COOPERATIVA DE AHORRO Y CRÉDITO ALIANZA DEL VALLE LTDA”, utilizará el estándar COBIT 4.0, para la evaluación y auditoria del ambiente informático de la Cooperativa Alianza del Valle, profundizando conceptos de control interno y procedimientos que se ejecutan.

## 2. METODOLOGÍA

Para la ejecución de este trabajo se utiliza la metodología ABR (Auditoria en base a riesgos), se fundamenta en el estándar internacional COBIT 4.0 y se desarrolla en las siguientes etapas:

- Planeación de la Auditoría.
- Desarrollo de la Auditoría.
- Emisión del Informe de Auditoría (Observaciones y Recomendaciones).

### 2.1 Planeación de la Auditoria

En esta fase se establecen las relaciones entre auditores y la entidad, para determinar 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 permiten 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 auditoria
3. Análisis Preliminar del Control Interno
4. Análisis de los Riesgos y la Materialidad
5. Planeación Específica de la auditoria
6. Elaboración de programas de  Auditoria

Con el fin de lograr el tratamiento más adecuado y seguro de la información, el contenido del plan de revisión de sistemas se resume como lo siguiente:

- Origen de la Auditoría
- Marco de Trabajo
- Alcance
- Desarrollo

### 2.1.1 Origen de la Auditoría

La revisión al área de sistemas y de los procesos por donde se encuentra relacionada la información, es un proceso indispensable a la hora de realizar servicios de Auditoría Informática, esta revisión tuvo por objeto ser soporte a la Auditoría Financiera y consultoría al cliente, para guiarlo en medidas de control interno, seguridades, utilización de hardware y software y el control de la calidad sobre la información.

### 2.1.2 Marco de Trabajo

Para la revisión de los sistemas de la Cooperativa de Ahorro y Crédito Alianza del Valle, se adoptó el Marco de trabajo recomendado por COBIT 4.0. (Como se muestra en la siguiente figura)

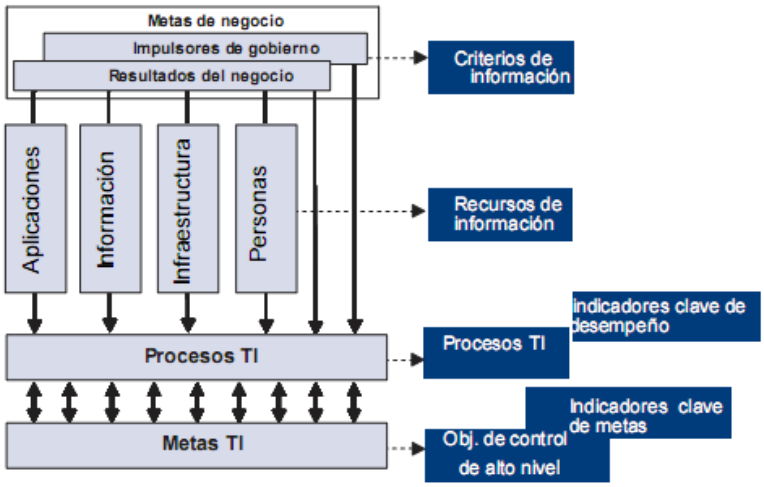


**Figura 1.** Marco del Trabajo COBIT 4.0.

### 2.1.3 Alcance

El alcance de la auditoría se realizó en base a COBIT 4.0 y está limitado a la Cooperativa de Ahorro y Crédito Alianza del Valle en el área de Sistemas en el periodo comprendido entre Agosto 1 del 2011 hasta Diciembre 28 del 2011.

### 2.1.4 Desarrollo

Se detalla lo que se analizó, métodos y demás particularidades que se toman en cuenta a la hora de realizar el trabajo. Incluyendo como valor agregado al proyecto, un pequeño análisis estadístico que determina el grado de satisfacción que poseen los usuarios de la entidad con respecto al sistema que utiliza.

## 2.2 Ejecución de la auditoria Informática

En la ejecución de la auditoria informática se recopiló la información necesaria en documentos y evidencias que permitieron al auditor fundamentar sus comentarios, sugerencias y recomendaciones con respecto al manejo y administración de TI.

Para la recolección de información se utilizaron diversas técnicas como:

- 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 pasó luego al análisis que se realizó utilizando un criterio profesional por parte de los auditores y el equipo a cargo del proceso de Auditoria, toda la información recopilada fue clasificada de manera que permita ubicarla fácilmente y justificar de manera correcta las recomendaciones.

La evidencia se clasifica de la siguiente manera:

. Evidencia documental.

b. Evidencia física.

c. Evidencia analítica.

d. Evidencia testimonial.

Una vez que se tuvo información real y confiable se procedió a evaluar y probar el diseño y aplicación de los controles en la organización, para esto el equipo de Auditoria utilizó medios informáticos y electrónicos que permiten obtener resultados reales.

Para dar una opinión favorable o no de un sistema o proceso informático, el equipo de auditores

comprobó el funcionamiento de los sistemas de aplicación y efectuó una revisión completa de los equipos de cómputo.

### 2.3 Finalización de la auditoria Informática

Para finalizar un proceso de Auditoria Informática se elaboró un informe que contiene conclusiones y recomendaciones necesarias para que la Cooperativa realice un mejoramiento continuo, esta documentación fue redactada por el equipo de Auditoria y entregó a la administración de la empresa para su evaluación y análisis.

En la lectura del informe borrador, la administración de la Cooperativa presentó sus puntos de vista en relación a las observaciones que se entregó por parte de las auditoras que las justificaron con las evidencias recolectadas durante todo el proceso.

El informe que presenta el grupo de Auditores contiene los siguientes puntos:

- El período de tiempo en el que se ha realizado la evaluación.
- El equipo de auditoría que ha intervenido en la evaluación indicando los integrantes y su experiencia en el campo de auditoría.
- Los objetivos que se pretendieron alcanzar con el proceso de auditoría.
- El estándar utilizado; en este caso al utilizar COBIT 4.0 se especificó los dominios que se utilizaron para la evaluación y el plan de trabajo realizado entregado a la administración.
- El criterio sobre el cual se está evaluando.
- La condición inicial en la que se encontró la Cooperativa.
- Describir las causas del estado actual de la organización, además se detalló las consecuencias que puede traer si la empresa continua manejándose de la misma forma.
- Detallar explicativamente las recomendaciones que se hacen a la administración y que 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.
- Incluir las opiniones y puntos de vista de la administración especificando si la organización va a adoptar o no las recomendaciones propuestas por el grupo de auditores.

## 3. MATERIALES Y MÉTODOS

En la realización de esta auditoría informática, las pruebas que se usaron son las que se describen a continuación:

- **Pruebas de cumplimiento:** Determinan si un sistema de control interno funciona adecuadamente (según la documentación, según declaran los auditados y según las políticas y procedimientos de la organización).
- **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, sea 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 trascripción de la observación (como se expresara la observación, por escrito, visualmente, etc.).

- **Cuestionarios.-** Es útil cuando la información propia es escasa y / o la unidad auditada se encuentra en una ubicación lejana. La información obtenida a través de él nos permite adelantar un pre diagnóstico, de la situación de la unidad y orienta el trabajo de campo. Este cuestionario ha de tener un diseño estándar, idéntico para todas las unidades a auditar, permitiendo así la comparación del estado de una unidad con otras o de esta misma unidad en diferentes instantes de tiempo.
- **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" tensión está en adoptar una postura amigable y de colaboración. El rendimiento 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.

## 4. DISEÑO E IMPLEMENTACIÓN

Existen varias posibilidades para enfrentar la auditoría según lo establecido por COBIT, y pueden ser:

- Controles de riesgo
- Pasos y Tareas
- Puntos de Decisión.

El esquema planteado para el presente trabajo corresponde a examinar los Pasos y Tareas, debido a que se revisaron los controles seleccionados para cada dominio y se evaluaron las actividades realizadas el sistema de información.

Otra decisión a tomada en este momento fué definir si la auditoría sería llevada a cabo con una metodología Cuantitativa o Cualitativa (Subjetiva).

En este caso se utilizó un método mayormente cualitativo, aunque en ciertos casos se utilizó análisis cuantitativo, ya que el enfoque con el que se trabaja está basado en la experiencia, concentrándose en factores intangibles.

## 5. RESULTADOS

La siguiente matriz muestra el estado o situación inicial en la que se encuentra la empresa nos ayuda a determinar los riesgos altos que deben ser auditados y mejorados.

Matriz de riesgos base para la investigación de campo.-

| | |
|---|---|
| | 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 | | |

**Resultados Oficiales:**

- La planificación no cuenta con planes tácticos; tampoco se ha realizado una evaluación de su cumplimiento; lo que dificulta una adecuada continuidad del negocio. Por esta razón es imperativo capacitar al Jefe del Departamento de Sistemas y al Auditor Interno en temas relacionados, que permita a La Cooperativa de Ahorro y Crédito Alianza del Valle, contar con planes en los niveles de calidad requeridos.
- Se debe implantar de forma inmediata un esquema de clasificación de datos que aplique a toda la empresa (pública, confidencial, secreta); al no tener un correcto esquema de clasificación de datos es imposible aplicar un sistema de seguridad eficaz y eficiente; esto puede ser causa de perjuicio

económico a la Cooperativa con alto riesgo en la protección de los datos críticos que no hayan sido considerados como tales.

- La Cooperativa Alianza del Valle no cuenta con una correcta administración de riesgos en TI; por este motivo el Jefe del Departamento de Sistemas debe implementar un esquema de administración de riesgos en base a un plan que considere: identificación y análisis de riesgos, riesgos e impacto a la funcionalidad de negocio, posibilidad de concurrencia, prioridad de riesgos, factores de minimización de impacto de riesgos definidos y nuevos, evaluación permanente de los riesgos.
- La adquisición de Infraestructura tecnológica no obedece a un plan previamente establecido, a pesar de que este plan es de gran importancia para la Cooperativa ya que permitirá el correcto cumplimiento de las metas del negocio, en escalabilidad, riesgos y vida útil de la inversión.
- El desarrollo, implantación y mantenimiento del software no se realiza en base de normas establecidas; no se cumple con procedimientos formales para la administración del software incumpliendo con políticas de permisos de acceso a códigos fuente. Esto hace necesario emprender en un proceso agresivo de capacitación al personal del departamento de informática en temas inherentes al desarrollo, mantenimiento y seguridad del software con normas de calidad.
- No se encuentra desarrollado e implementado un proceso para registrar, evaluar y dar prioridad en forma consistente a las solicitudes de cambio, lo que da lugar a la degradación del software por tener cambios sin registrar; se debe establecer un proceso de administración de cambios que se revise con regularidad.
- No se evidencia una gestión de servicios informáticos acorde al tamaño y las necesidades funcionales de la Cooperativa Alianza del Valle; en las encuestas a los usuarios internos se ha determinado que el apoyo informático no es eficiente; este factor ha deteriorado la comunicación entre usuarios y prestadores de servicio; por tanto es necesario implementar un marco de trabajo que defina la estructura organizacional para la administración del nivel de servicio, incluyendo roles, tareas y responsabilidades de los proveedores externos, internos y de los clientes.
- La configuración de la red del Core Bancario Cobis no se ha actualizado; existen servidores de agencia que se encuentran registrados sin su existencia física. Se pudo evidenciar que la administración de datos no es adecuada, ya que no han sido compactados ni depurados, es imprescindible que se revise las configuración de la red para mejorar la seguridad del servidor central, eliminando registros de servidores inexistentes; se debe realizar una depuración periódica de tablas y un correcta compactación de datos para mejorar el manejo de las mismas.
- La Cooperativa no cumple con una administración de la base de datos SYBASE acorde con políticas de monitoreo de servidores, revisión de consistencia de base de datos, bitácoras para el registro de sucesos y permisos de acceso de los usuarios, por este motivo es necesario cumplir con las normas de administración de base de datos que se encuentran estipuladas.
- No se pudo evidenciar el cumplimiento del manual para ejecución de pruebas ni documentos que validen la actualización del plan de contingencia en transición.

- En el análisis de las seguridades físicas se pudo constatar, que los data center no cuentan con un adecuado control de acceso, poseen cámaras que no están debidamente monitoreadas, su personal no cuenta con capacitación en el uso de los extintores; no poseen pisos falsos ni otros dispositivos que mitiguen el riesgo de daño en los equipos en caso de inundación.

## 6. TRABAJOS RELACIONADOS.

Existen otros trabajos realizados con anterioridad y que fueron revisados por parte del equipo de auditoría como: Evaluación de las Seguridades y redes de la Cooperativa, ejecutado por una empresa consultora.

## 7. CONCLUSIONES Y TRABAJO FUTURO

La auditoría realizada presenta las debilidades en los aspectos definidos por la matriz de riegos, con las evidencias obtenidas de las actividades de verificación de los controles especificadas en la norma Internacional COBIT, en base a una metodología de Auditoría en Base de Riesgos (ABR), detallada en un Plan de investigación de campo y ejecutada con instrumentos de evaluación acordes con el objetivo de investigación.

Es importante que las recomendaciones sean acogidas por la Administración de la Cooperativa y se disponga la elaboración de un plan de cumplimiento, el que deberá estar en concordancia con el Plan Estratégico y Plan Operativo de la Institución.

## 8. AGRADECIMIENTOS

Los autores, expresarán su reconocimiento y agradecimiento a quienes hicieron posible la ejecución de esta tesis: los miembros de la administración de la Cooperativa de Ahorro y Crédito Alianza del Valle, a los directores de la tesis, quienes aportaron con su experiencia en la dirección de la misma.

## 9. REFERENCIAS BIBLIOGRÁFICAS

[1] ISO 27002 y COBIT 4.0 Disponible en: www.monografias.com

[2] Resolución y decretos, Disponible en: http://www.sbs.gob.ec/

[3] Manual de Auditoría; Proporcionada por una firma de Auditoría, Edición del 2008.

[4] José Antonio Echenique García, “Auditoria Informática”, Editorial McGraw-Hill. Segunda Edición.

[5] Murphy, David, “La auditoría de sistemas informáticos, (1998)

[6] Gil Peuchan Ignacio, “Sistemas y Tecnologías de la Información para la Gestión”, Edit. McGraw Hill, Madrid-España (1999),

[7] Sergio Etcheverry, “Auditoria a las Tecnologias de la Informacion”, http://www.unap.cl/~setcheve/ati/DefinirunaPlanEstratgicoenTI.html