UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

La Universidad Católica de Loja

MODALIDAD PRESENCIAL

Auditoría Informática orientada a los procesos críticos de crédito generados en la Cooperativa de Ahorro Y Crédito "Fortuna" aplicando el marco de trabajo COBIT

TESIS DE GRADO PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN SISTEMAS INFORMÁTICOS Y COMPUTACIÓN

AUTOR:

Karolay Michell Coronel Castro

DIRECTOR:

Ing. Marco Patricio Abad Espinoza

CO-DIRECTORA:

Ing. Samanta Patricia Cueva Carrión

Loja- Ecuador
2012

CERTIFICACIÓN

Ingeniero.
Marco Patricio Abad Espinoza.

DOCENTE INVESTIGADOR DE LA ESCUELA DE CIENCIAS DE LA COMPUTACIÓN DE LA UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA.

CERTIFICA:

Haber dirigido y supervisado el desarrollo del presente proyecto de tesis con el tema ***"Auditoría Informática Orientada a los Procesos Críticos de Crédito generados en la Cooperativa de Ahorro y Crédito "Fortuna" aplicando el Marco de Trabajo COBIT*** *previo a la obtención del título de* ***INGENIERA EN SISTEMAS INFORMÁTICOS Y COMPUTACIÓN****, y una vez que este cumple con todas las exigencias y los requisitos legales establecidos por la Universidad Técnica Particular de Loja, autoriza su presentación para los fines legales pertinentes.*

_____

Ing. Marco Patricio Abad Espinoza.

DIRECTOR DE TESIS

CERTIFICACIÓN

Ingeniera.
Samanta Patricia Cueva Carrión.

DOCENTE INVESTIGADOR DE LA ESCUELA DE CIENCIAS DE LA COMPUTACIÓN DE LA UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA.

CERTIFICA:

Haber dirigido y supervisado el desarrollo del presente proyecto de tesis con el tema ***"Auditoría Informática Orientada a los Procesos Críticos de Crédito generados en la Cooperativa de Ahorro y Crédito "Fortuna" aplicando el Marco de Trabajo COBIT*** *previo a la obtención del título de* ***INGENIERA EN SISTEMAS INFORMÁTICOS Y COMPUTACIÓN****, y una vez que este cumple con todas las exigencias y los requisitos legales establecidos por la Universidad Técnica Particular de Loja, autoriza su presentación para los fines legales pertinentes.*

_____

Ing. Samanta Patricia Cueva Carrión.

CO-DIRECTORA DE TESIS

AUTORÍA

El presente proyecto de tesis con cada una de sus observaciones, análisis, evaluaciones, conclusiones y recomendaciones emitidas, es de absoluta responsabilidad del autor.

Además, es necesario indicar que la información de otros autores empleada en el presente trabajo está debidamente especificada en fuentes de referencia y apartados bibliográficos.

.....

Karolay Michell Coronel Castro

Autor

CESIÓN DE DERECHOS

Yo, Karolay Michell Coronel Castro, declaro ser autor del presente trabajo y eximo expresamente a la Universidad Técnica Particular de Loja y a sus representantes legales de posibles reclamos o acciones legales.

Adicionalmente declaro conocer y aceptar la disposición del Art. 67 del Estatuto Orgánico de la Universidad Técnica Particular de Loja que su parte pertinente textualmente dice: "Forman parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través, o con el apoyo financiero, académico o institucional (operativo) de la Universidad".

.....

Karolay Michell Coronel Castro

Autor

DEDICATORIA

Me gustaría dedicar esta Tesis a toda mi familia.

A mi esposo Juan Carlos, a él especialmente le dedico esta Tesis por su ayuda, por su paciencia, por su comprensión, por su empeño, por sus ánimos, por su amor, por ser tal y como es. Realmente él me llena por dentro para conseguir un equilibrio que me permita dar el máximo de mí. Nunca le podré estar suficientemente agradecida.

A mi hijo Nicolas Sebastián, quien han sido mi fuerza, mi soporte y por quien todo esfuerzo y sacrificio vale la pena. Él es la persona que más directamente ha sufrido las consecuencias del trabajo realizado. Es sin duda mi referencia para el presente y para el futuro.

A mi madre Melvita, cuyo respaldo y ejemplo han sido fundamentales en mi formación no solo académica sino también ética y moral; ella me ha enseñado a encarar las adversidades sin perder nunca la dignidad ni desfallecer en el intento. Me ha dado todo lo que soy como persona, mis valores, mis principios, mi perseverancia y mi empeño, y todo ello con una gran dosis de amor y sin pedir nunca nada a cambio. A ella quien me enseño a ser constante, responsable y sobre todo a esforzarme para lograr cumplir las metas que me proponga en la vida, sin dejarme vencer por las adversidades que se presentaron en el trayecto.

Karolay Michell Coronel Castro

Autor

AGRADECIMIENTO

A Dios que todo lo permite, dándome fortaleza y perseverancia para culminar con este sueño anhelado.

A los ingenieros Patricio Abad, Director de Tesis, y Samanta Cueva, Co-directora de Tesis, quienes aportaron con su dirección y conocimiento para cumplir con esta meta.

A la Cooperativa de Ahorro y Crédito "Fortuna ", que permitió efectuar éste trabajo en sus instalaciones.

A mis compañeras de la Cooperativa de Ahorro y Crédito "Fortuna", por los ánimos y palabras de aliento brindadas en todo momento difícil del desarrollo de mi tesis.

A mis amigos de la Universidad, por compartir sus conocimientos conmigo, por haber dedicado parte de su apretado tiempo a ayudarme, por sus ánimos y apoyo brindados en los momentos malos y en los menos malos.

A todos quienes de una u otra forma apoyaron desinteresadamente al desarrollo de este proyecto.

A todos ellos, muchas gracias.

ÍNDICE DE CONTENIDOS

CERTIFICACIÓN ii
CERTIFICACIÓN iii
AUTORÍA iv
CESIÓN DE DERECHOS v
DEDICATORIA vi
AGRADECIMIENTO vii
ÍNDICE DE CONTENIDOS viii
ÍNDICE DE FIGURAS xi
ÍNDICE DE TABLAS xii
RESUMEN 1
INTRODUCCIÓN 2
OBJETIVOS 3
General 3
Específicos 3
METODOLOGÍA 3
RESULTADOS ESPERADOS 4
ESTRUCTURA DE LA TESIS 4
ESTRATEGIA DE EJECUCIÓN 5
CAPÍTULO 1: 9
1. EL PROCESO DE LA AUDITORÍA INFORMÁTICA 10
1.1. AUDITORÍA INFORMÁTICA 10
1.1.1. DEFINICIÓN 10
1.1.2. ALCANCE 10
1.1.3. TIPOS DE AUDITORÍA INFORMÁTICA 10
1.1.4. METODOLOGÍAS DE AUDITORÍA INFORMÁTICA 11
1.1.5. PRINCIPALES PRUEBAS Y HERRAMIENTAS PARA EFECTUAR UNA AUDITORÍA INFORMÁTICA 12
1.1.6. PROCESO DE UNA AUDITORÍA INFORMÁTICA 12
1.1.7. ESTÁNDARES DE AUDITORÍA INFORMÁTICA 14
1.2. AUDITORÍA INFORMÁTICA EN EL SECTOR BANCARIO 16
1.2.1. NECESIDAD Y BENEFICIOS DE LA AUDITORÍA INFORMÁTICA EN LAS ENTIDADES FINANCIERAS 16
1.2.2. AUDITORÍA INFORMÁTICA EN LA PROTECCIÓN DE DATOS PERSONALES 16
1.2.3. ACTIVIDADES DE AUDITORÍA EN RELACIÓN CON LA PROTECCIÓN DE DATOS PERSONALES 17
1.3. EJEMPLOS DE APLICACIÓN 17
1.4. COBIT COMO MARCO DE REFERENCIA PARA AUDITORÍA INFORMÁTICA 20
1.4.1. ESTRUCTURA DEL MARCO REFERENCIAL COBIT 20
1.4.2. DOMINIOS 21
1.4.2.1. PLANEAR Y ORGANIZAR (PO) 21
1.4.2.2. ADQUIRIR E IMPLEMENTAR (AI) 22

1.4.2.3. ENTREGAR Y DAR SOPORTE (DS) 22
1.4.2.4. MONITOREAR Y EVALUAR (ME) 22
1.4.3. OBJETIVOS DE CONTROL 23
1.4.4. MODELOS DE MADUREZ 24
CAPÍTULO 2: 26
2. ANÁLISIS SITUACIONAL DE LA COOPERATIVA DE AHORRO Y CRÉDITO "FORTUNA" 27
2.1. DEFINICIÓN DE LA PROBLEMÁTICA 27
2.2. ANTECEDENTES 27
2.3. INFORMACIÓN INSTITUCIONAL 28
2.3.1. DESCRIPCIÓN DE LA EMPRESA 28
2.3.2. MISIÓN 29
2.3.3. VISIÓN 29
2.3.4. VALORES 29
2.3.5. OBJETIVOS INSTITUCIONALES 29
2.3.6. PRODUCTOS Y SERVICIOS 30
2.3.7. INFRAESTRUCTURA 31
2.3.8. ORGANIGRAMA ESTRUCTURAL 31
2.3.8.1. DEPARTAMENTO DE SISTEMAS 32
2.3.8.2. DEPARTAMENTO DE CRÉDITO 32
2.4. ESTRATEGIA GENERAL 33
2.4.1. ANTECEDENTES 33
2.4.2. ALCANCE 33
2.4.3. EQUIPO AUDITOR 33
2.4.4. INVOLUCRADOS 33
2.5. PROCESOS DE CRÉDITO EN LA COOPERATIVA 33
"FORTUNA" 33
2.5.1. PROCESOS PARA OTORGAR CRÉDITOS A LOS SOCIOS 35
2.5.1.1. PRIMER PROCESO (PC1): ANÁLISIS DEL CRÉDITO 35
2.5.1.2. SEGUNDO PROCESO (PC2): APROBACIÓN DEL CRÉDITO 38
2.5.1.3. TERCER PROCESO (PC3): LEGALIZACIÓN DEL CRÉDITO 40
2.5.1.4. CUARTO PROCESO (PC4): DESEMBOLSO DEL CRÉDITO 42
2.5.1.5. QUINTO PROCESO (PC5): RECUPERACIÓN DEL CRÉDITO 44
2.6. PROCESOS COBIT QUE SE APLICARÁN EN LA AUDITORÍA 47
CAPÍTULO 3: 50
3. APLICACIÓN DE LA AUDITORÍA INFORMÁTICA 51
3.1. DISEÑO DE INSTRUMENTOS 51
3.2. ESTUDIO Y SELECCIÓN DE HERRAMIENTAS DE VALIDACIÓN 56
3.3. PROCESO DE LA AUDITORÍA 56
3.3.1. APLICACIÓN DE NESSUS 58
3.3.2. APLICACIÓN DE IDEA 70
3.3.3. APLICACIÓN DE LOS MODELOS DE MADUREZ 87
3.5.1. HALLAZGOS DE LA AUDITORÍA 89

CAPÍTULO 4: 95
4. RESULTADOS DE LA AUDITORÍA INFORMÁTICA 96
4.1. ANÁLISIS DE RESULTADOS 96
4.2. DEFINICIÓN DE OPORTUNIDADES DE MEJORA 102
4.3. PLAN DE ACCIÓN 104
CONCLUSIONES Y RECOMENDACIONES 110
CONCLUSIONES 110
RECOMENDACIONES 111
GLOSARIO 112
BIBLIOGRAFÍA 117
LISTA ANEXOS 122
ANEXOS 126
PAPER 127

ÍNDICES

ÍNDICE DE FIGURAS

Figura 1.1. Proceso del Operativo de Auditoría *13*
Figura 1.2. Cubo COBIT. ... *20*
Figura 1.3. Los cuatro dominios de COBIT ... *21*
Figura 1.4. Representación gráfica de los modelos de madurez ... *24*
Figura 2.1. Organigrama Estructural de la Cooperativa de Ahorro y Crédito "Fortuna". ... *32*
Figura 2.2. Diagrama SIPOC del proceso de Análisis del Crédito. ... *38*
Figura 2.3. Diagrama SIPOC del proceso de Aprobación del Crédito. ... *40*
Figura 2.4. Diagrama SIPOC del proceso de Legalización del Crédito. ... *42*
Figura 2.5. Diagrama SIPOC del proceso de Desembolso del Crédito. ... *44*
Figura 2.6. Diagrama SIPOC del proceso de Recuperación del Crédito. ... *46*
Figura 3.1. Proceso de la Auditoría ... *58*
Figura 3.2.Componentes de NESSUS. ... *58*
Figura 3.3. Pantalla principal de NESSUS. ... *60*
Figura 3.4. Ventana principal con plugins obtenidos. ... *61*
Figura 3.5. Proceso de creación de un nuevo usuario. ... *62*
Figura 3.6. Ingreso a NESSUS Client. ... *63*
Figura 3.7. Política creada para la cooperativa "Fortuna". ... *63*
Figura 3.8.Información de Credentials. ... *64*
Figura 3.9. Información de Plugins. ... *64*
Figura 3.10. Selección de tipo de base de datos en Preferences. ... *65*
Figura 3.11. Creación de nuevo scan. ... *65*
Figura 3.12. Información de scan realizado. ... *66*
Figura 3.13. Información de vulnerabilidades encontradas. ... *66*
Figura 3.14. Obtención del reporte de vulnerabilidades ... *67*
Figura 3.15. Componentes de IDEA. ... *71*
Figura 3.16. Ventana principal de IDEA. ... *72*
Figura 3.17. Asistente de importación ... *73*
Figura 3.18. Importación de la base de datos ... *73*
Figura 3.19. Archivo de importación. ... *74*
Figura 3.20. Opción Extracción Directa. ... *75*
Figura 3.21. Fórmula para obtener el monto límite de Crédito Comercial y Consumo. ... *76*
Figura 3.22. Resultados de límites elevados. ... *76*
Figura 3.23. Opción Comparar Bases de Datos. ... *77*
Figura 3.24. Calculo de mora en nueva base de datos. ... *78*
Figura 3.25. Proceso de comparación de dos bases de datos. ... *78*
Figura 3.26. Resultados de la comparación del campo mora. ... *79*
Figura 3.27. Opción Sumarización. ... *80*
Figura 3.28. Proceso de Sumarización ... *80*
Figura 3.29. Resultados de clientes demandados. ... *81*
Figura 3.30. Opción Clave Duplicada. ... *82*
Figura 3.31. Resultado de la verificación de claves repetidas. ... *82*
Figura 3.32. Fórmula para verificar operaciones el día domingo. ... *83*
Figura 3.33. Extracción de datos dada la formula. ... *83*

Figura 3.34. Resultados de operaciones en día Domingo. *84*
Figura 3.35. Opción Detección de Omisiones. *85*
Figura 3.36. Proceso de detección de omisiones. *86*
Figura 3.37. Resultados de detección de omisiones *86*
Figura 3.38. Comparativa de los niveles de madurez vs dominios COBIT. *89*
Figura 4.1. Cronograma de Actividades del Plan de Acción *105*

ÍNDICE DE TABLAS

Tabla 1.1. Tipos de Auditoría Informática [4] *11*
Tabla 1.2. Cuadro comparativo entre COBITT, ITIL y la ISO 27000. ..... *14*
Tabla 2.1. Matriz de Probabilidad de Ocurrencia de un Proceso de Crédito *34*
Tabla 2.2. Procesos de Crédito a Auditar. *34*
Tabla 2.3. Relación entre procesos de crédito y dominios COBIT. *49*
Tabla 3.1. Parámetros de configuracion de NESSUS. *59*
Tabla 3.2. Detección de vulnerabilidades en el servidor de Base de Datos y servidor DNS. *67*
Tabla 3.3. Detección de vulnerabilidades en los equipos del área de crédito. *69*
Tabla 3.4. Tipos de créditos *74*
Tabla 3.5. Nivel de Madurez del Dominio PLANEAR Y ORGANIZAR *88*
Tabla 3.6. Nivel de Madurez del Dominio ADQUIRIR E IMPLEMENTAR *88*
Tabla 3.7. Nivel de Madurez del Dominio ENTREGAR Y DAR SOPORTE *88*
Tabla 3.8. Nivel de Madurez del Dominio MONITOREAR Y EVALUAR. *89*
Tabla 3.9. Matriz de Medición de Criticidad. *90*
Tabla 3.10. Hallazgos de la Auditoría Informática. *90*
Tabla 4.1. Fortalezas encontradas luego de realizada la Auditoría Informática. *96*
Tabla 4.2.Debilidades en cuanto a políticas y procedimientos luego de realizada la Auditoría Informática. *98*
Tabla 4.3.Debilidades en cuanto a seguridad física luego de realizada la Auditoría Informática. *99*
Tabla 4.4.Debilidades en cuanto al sistema luego de realizada la Auditoría Informática. *100*
Tabla 4.5.Debilidades en cuanto a servidores luego de realizada la Auditoría Informática. *101*
Tabla 4.6.Propuesta Económica de Dispositivos. *103*
Tabla 4.7.Propuesta Económica de Software. *103*
Tabla 4.8. Plan de Acción. *106*
Tabla 4.9. Presupuesto del plan de acción. *108*

Karolay Coronel

RESUMEN

La presente investigación se enfoca al desarrollo del proceso de una auditoría informática para evaluar y determinar el nivel de cumplimiento de los procesos críticos de crédito de la Cooperativa de Ahorro y Crédito “Fortuna”, en base al marco de referencia COBIT. El proceso abarca la recopilación de la mayor cantidad de evidencia técnica mediante la aplicación dos herramientas: IDEA para análisis de la base de datos y NESSUS para escaneo de vulnerabilidades de equipos, también se aplicó la metodología de los modelos de madurez del COBIT, la cual por medio de una matriz de evaluación permitió la verificación del cumplimiento de los procesos de crédito, todo esto con el fin de emitir un informe de hallazgos, que muestre las falencias existentes en dichos procesos, tanto manuales como sistematizados. Finalmente se plantea un plan de acción el cual pretende facilitar la toma de decisiones por parte de los directivos de institución, el cual asociado a la introducción y consolidación de la auditoría informática establecerá una cultura de seguridad en el tratamiento de la información en todos los procesos de negocio.

INTRODUCCIÓN

Según Pilar Amador Contra [1], una de las tareas clásicas en cualquier actividad auditora es la relacionada con las funciones de control, ya que se debe verificar la existencia de procedimientos y mecanismos de control suficientes y adecuados que permitan asegurar el correcto funcionamiento de los sistemas informáticos y principalmente evaluar la implicación de la inexistencia, la insuficiencia y la no adecuación de dichos procedimientos, todo esto con el fin de asegurar que las aplicaciones informáticas cumplan con los criterios funcionales definidos por la entidad financiera.

La importancia de la tecnología de información dentro de una organización financiera juega en la actualidad uno de los papeles más relevantes, pues brindan un soporte indispensable a los procesos críticos de la institución y permite la toma de acciones correctivas para el progreso del negocio, por lo cual es fundamental que se preste un correcto seguimiento de las políticas y procedimientos establecidos dentro de la organización.

Durante el desarrollo del trabajo se define la problemática, se establece el plan de auditoría informática, el cual contempla el objetivo principal, el alcance de la auditoría, quién va realizar la auditoría, qué personas estarán involucradas y la elaboración del informe final de la ejecución de la auditoría informática.

La principal preocupación que ha surgido en la cooperativa de Ahorro y Crédito "Fortuna", es que los procesos correspondientes a los productos y servicios que se generan diariamente puedan estar obsoletos o que no exista el control adecuado para verificar su funcionamiento, haciéndose necesario realizar una auditoría a los procesos de crédito, al sistema informático "CONEXUS" y de TI (Tecnología de la Información), así como el cumplimiento de las normativas que rigen dichos procesos.

Para el desarrollo de éste tema se busco una de las mejores prácticas de auditoría informática, que sea factible de implementar y que permita generar resultados confiables, tomando en cuenta las condiciones de la institución, es por ello que se optó por COBIT (Objetivos de Control para Tecnología de Información y Tecnologías relacionadas,) ya que cumple con los requerimientos antes mencionados.

OBJETIVOS

El propósito de este trabajo de investigación es cumplir con los objetivos propuestos, a continuación se definen los siguientes:

General

Aplicar auditoría informática para evaluar y determinar el nivel del cumplimiento de los procesos críticos de crédito generados en la Cooperativa de Ahorro y Crédito "Fortuna", en base al marco de referencia COBIT.

Específicos

Los objetivos específicos son los siguientes:

- Estudio de los procesos del marco de trabajo COBIT.
- Establecer el grado de madurez actual de acuerdo con los modelos de madurez de COBIT.
- Conocer los procedimientos crediticios internos de la cooperativa.
- Auditar el funcionamiento del sistema informático con respecto a los procesos de crédito.
- Analizar, verificar y controlar la existencia de seguridad, eficiencia y calidad de la información crediticia del sistema informático de la cooperativa.
- Estudio y determinación del grado de confianza a depositar en el sistema informático de la cooperativa.
- Generar recomendaciones y un plan de acción con las posibles mejoras que se puedan realizar tanto a los procesos manuales como informáticos, para mejorar así el manejo de la información crediticia.
- Elaborar el Informe de la auditoría informática considerando todo los hallazgos encontrados.

METODOLOGÍA

La metodología aplicada en el desarrollo de la tesis es la siguiente:

- Lectura y estudio, de conceptualización y análisis de información relacionada.
- Análisis comparativo de posibles herramientas y controles de implementación en la auditoría informática.
- Investigación de una metodología aplicable al ámbito de entidades financieras y dando un enfoque principal a la cooperativa" Fortuna" basado en COBIT.

- Aplicación de la metodología investigada (COBIT).
- Conclusiones.
- Propuesta de acciones de control y mejora en los procesos de crédito.
- Presentación del informe final.

RESULTADOS ESPERADOS

Al finalizar la investigación de auditoría aplicada a los procesos de crédito de la cooperativa de Ahorro y Crédito "Fortuna", la cual está siendo desarrollada en base a la identificación y aplicación de los procesos correspondientes a los cuatro dominios del marco de referencia COBIT los mismos que tendrán relación con los procesos de crédito que se aplican en la cooperativa, se obtendrán los siguientes resultados:

- Pautas que permitan guiar el análisis de la información generada por la auditoría informática.
- Un informe con los resultados de la auditoría informática aplicada a los procesos de crédito y desarrollada en la Cooperativa de Ahorro y Crédito "Fortuna".
- Recomendaciones obtenidas en base a la investigación.
- Plan de acción a tomarse de acuerdo a la metodología investigada COBIT.

ESTRUCTURA DE LA TESIS

La presente auditoría orientada a los procesos críticos de crédito de la cooperativa de Ahorro y Crédito "Fortuna" está estructurada en cuatro capítulos, que se mencionan a continuación:

En la sección inicial se define la introducción, definición del problema, objetivos, metodología y resultados esperados de la tesis.

Luego en el capítulo 1, se revisa el proceso de la auditoría informática, en esta fase se plantea el marco teórico base para el desarrollo de este trabajo, primeramente con los conocimientos generales de la auditoría informática su definición, objetivos, importancia, alcance, tipos, metodologías, funciones, pruebas y herramientas de una auditoría informática, el proceso de una auditoría informática, controles, análisis de riesgos, entre otros aspectos; y, la sección correspondiente al estándar COBIT, definición, misión, objetivos, principios, beneficios, marco de trabajo, estructura, dominios, los objetivos de control y modelos de madurez de cada proceso, finalizando con ejemplos de aplicación.

En el capítulo 2, se realiza el análisis situacional acerca de la Cooperativa de Ahorro y Crédito "Fortuna" como antecedentes, información institucional, descripción de la empresa, objetivos institucionales, productos y servicios, infraestructura, organigrama institucional, estrategia general, detalle de los procesos de crédito, diagramas SIPOC de los procesos de créditos, selección de los procesos de los dominios del COBIT a aplicar.

En el capítulo 3, se realiza la aplicación de la auditoría informática, en esta fase, se realiza la ejecución de la auditoría informática iniciando por el diseño de instrumentos a utilizar, el estudio y selección de herramientas de validación, la aplicación de la auditoría informática en base a las herramientas y metodología estudiadas, la verificación de las evidencias en base a una matriz de evaluación, y el informe de resultados detallando los hallazgos de la auditoría.

Finalmente en el capítulo 4, se presenta los resultados de la auditoría informática, en donde se analizan los productos obtenidos de la auditoría, se define una oportunidad de mejora para la cooperativa y una se elabora el plan de acción en base a los hallazgos más significativos de la auditoría con sus respectivas recomendaciones, además se emite el informe final de la auditoría informática a la cooperativa "Fortuna".

Para culminar se emiten las conclusiones y recomendaciones más relevantes de éste trabajo de tesis.

ESTRATEGIA DE EJECUCIÓN

Al ser el marco de trabajo COBIT la metodología en la que se basará el presente proyecto, es necesario mencionar que ha sido escogida principalmente por su facilidad de adaptación a cualquier tipo de negocio, por lo que no presentará ninguna dificultad para la revisión de los sistemas de información de la cooperativa de ahorro y crédito "Fortuna", además que COBIT (Control Objectives For Information anRelated Technology), es un modelo desarrollado basándose en las mejores prácticas de seguridad tecnológica, administración y control de la tecnología de la información (TI).

Los objetivos principales del proceso de una auditoría informática son salvaguardar los activos, asegurar la integridad de los datos, la consecución de los objetivos gerenciales, y la utilización de los recursos con eficiencia y eficacia, para ello se debe realizar la recolección y evaluación de evidencias, pero este es un trabajo que se debe efectuar de manera organizada siguiendo procedimientos ordenados, a los que se los dividió en las siguientes fases:

1) Planificación de la auditoría informática
2) Ejecución de la auditoría informática
3) Finalización de la auditoría informática, las cuales se detallan a continuación.

Es importante la participación de todas las áreas involucradas en la auditoría a la cooperativa durante las fases del proyecto de la misma puesto que son una pieza fundamental para alcanzar los objetivos de ésta.

1) Planificación de la auditoría informática

Como todo proyecto implantado dentro de una organización, el proyecto de auditoría informática a los procesos críticos de crédito generados en la Cooperativa de Ahorro y Crédito "Fortuna" iniciara con una fase de planeación en la cual participaran las áreas de gerencia,

crédito y sistemas, con la finalidad de identificar los recursos necesarios que permitirán llevar a cabo este proyecto, como son, objetivos que se pretenden alcanzar con el proyecto, análisis costo/beneficio, personal humano que intervendrá en el proyecto, marco de referencia de auditoría informática que se va a utilizar (COBIT), basándose en varios objetivos fundamentales como:

- Evaluación de los sistemas y procedimientos.
- Evaluación del proceso de datos.
- Evaluación de las seguridades

Esta fase se resume en obtener un conocimiento inicial de la cooperativa, con especial énfasis en sus procesos crediticios e informáticos basados en evaluaciones administrativas realizadas a los procesos electrónicos, sistemas y procedimientos, seguridad y confidencialidad de los datos y aspectos legales de los sistemas y de la información obteniendo así una selección adecuada de los dominios del marco de referencia COBIT acorde a los procesos de crédito.

Una vez que se ha obtenido un conocimiento inicial de la cooperativa se procederá a establecer metas, programas de trabajo de auditoría, personal que intervendrá en el proyecto, y las fechas y la manera como se presentarán el informe de las actividades de cumplimiento del proyecto, basados en la realidad de la Cooperativa de Ahorro y Crédito "Fortuna".

También dentro del proceso de planificación de la auditoría informática se incluirá y documentara:

- Los objetivos y el alcance del trabajo.
- El relevamiento de información de las actividades a auditarse en la que se apoyará el análisis.
- Los recursos que se necesitarán para llevar a cabo el proyecto de auditoría.
- Los canales de comunicación necesarios entre los involucrados en el proyecto de auditoría.
- El procedimiento apropiado a utilizarse para realizar una inspección física que permita la obtención del conocimiento de la manera como se ejecutan las actividades y controles a auditar, así como de las áreas críticas en las que se debe poner mayor énfasis al realizar la auditoría.
- La aprobación del plan de trabajo de auditoría.

2) Ejecución de la auditoría informática

En la ejecución de la auditoría informática se hará la recolección de información y evidencias suficientes, para fundamentar los comentarios, conclusiones y recomendaciones, para lo cual se podrán utilizaran diversas técnicas como las siguientes:

- Entrevistas
- Cuestionarios (listas de chequeo)
- Observación directa

- Análisis de la información documental entregada por el auditado (evidencias)
- Paquetes de auditoría (generadores de programas).
- Revisión y análisis de la información de auditorías anteriores
- Revisión y evaluación de controles y seguridades.
- Metodología de los modelos de madurez del marco de trabajo COBIT

En el análisis de esta información será utilizado el criterio profesional adquirido por la experiencia de lo aprendido en el marco teórico, por medio de las encuestas aplicadas, las evidencias obtenidas claras y suficientes para comprobar el adecuado conocimiento de la entidad.

Los tipos de evidencias a usarse serán evidencia documental, física, analítica, y testimonial.

Una vez que se haya recolectado información confiable sobre la cual se pueda evaluar a la cooperativa, se procederá a probar la manera en la que han sido diseñados los controles, para esto se realizaran diagramas de flujo por los procesos de crédito con los cuales se verificará la información procesada por medios electrónicos y utilizarán métodos especializados de informática.

Se tomará en cuenta que para dar una opinión favorable acerca de los sistemas y determinar su confiabilidad en el procesamiento de la información, será necesario efectuar una revisión de los controles generales del computador, puesto que en la confiabilidad de ellos se basa el buen funcionamiento de los sistemas de aplicación.

3) Finalización de la auditoría informática

El resultado de la auditoría Informática, se materializará en un informe de conclusiones que será redactado y entregado a la administración de la cooperativa para su evaluación, por lo que antes de la emisión del informe final se deberán realizar varios borradores, que serán analizados en conjunto con la administración de la institución, para descubrir fallos en la evaluación de la auditoría posiblemente debido a otras interpretaciones acerca de la entidad.

La estructura del informe de conclusiones a entregarse a la administración de la cooperativa sería la siguiente:

- Iniciará con el período de tiempo en el que se ha realizado la evaluación.
- Se indicará el equipo de auditoría que ha intervenido en la evaluación.
- Se incluirán los objetivos que se pretendieron alcanzar con la evaluación de auditoría.
- Posteriormente se indicará los dominios de los cuales se ha realizado la evaluación de auditoría de acuerdo al marco de trabajo que utilizado, en este caso COBIT.
- Se indicará el criterio sobre el cual se ha realizado la evaluación, en este caso el criterio recomendado por los objetivos de control definidos en COBIT.
- Identificar la condición en la que se encontró a la cooperativa, o también conocida como observación.
- Se identificarán las causas que provocan la situación observada en la cooperativa.

- Se incluirá los efectos que puede provocar el hecho de que se mantenga la situación actual identificada por la auditoría en la cooperativa.
- Se incluirán las recomendaciones que la administración debería adoptar para cumplir con el criterio de los objetivos de control, que permita reducir la posibilidad de ocurrencia de los efectos anotados anteriormente.
- Por último incluirá el punto de vista de la administración en la que se indique si tomarán en cuenta las recomendaciones emitidas y las fechas en las cuales estas serán adoptadas, lo cual facilitará la ejecución de un seguimiento posterior de la auditoría.

En el informe final a ser presentado a la administración se incluirán solo los hechos importantes encontrados, puesto que la inclusión de objetivos irrelevantes no representa valor a la evaluación.

Cabe mencionar que la presente estrategia está sujeta a cambios que se puedan dar conforme avance el proceso de auditoría.

CAPÍTULO 1:

EL PROCESO DE LA AUDITORÍA INFORMÁTICA

1. *EL PROCESO DE LA AUDITORÍA INFORMÁTICA*

En el presente capítulo se realiza un análisis teórico sobre el tema de auditoría informática, su definición, sus objetivos, importancia, análisis de riesgos, controles internos, metodología, sus funciones, sus tipos y herramientas, la planeación de la auditoría finalizando con el conocimiento del informe final de la auditoría y una sección de auditoría informática en el sector bancario, que abarca temas relacionados al proceso de crédito de la cooperativa.

Además también se realiza el análisis teórico de lo que engloba este trabajo de tesis que es el marco de trabajo COBIT, conocer los dominios y sus procesos, los objetivos de control y sus respectivos modelos de madurez que permitirán posteriormente analizar la situación en la que se encuentra la Cooperativa de Ahorro y Crédito "Fortuna" en cuanto a los procesos de crédito. Finalmente se describe algunos ejemplos de aplicación que están basados en el estudio y aplicabilidad del marco de referencia COBIT.

Tanto los temas de auditoría informática como de COBIT son parte fundamental para el desarrollo de este trabajo de investigación, para tomarlo como una guía inicial en el desarrollo de la auditoría informática.

1.1. AUDITORÍA INFORMÁTICA

1.1.1. DEFINICIÓN

J.J. Acha define auditoría informática como "un conjunto de procedimientos y técnicas para evaluar y controlar total o parcialmente un sistema informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existente en cada empresa y para conseguir la eficacia exigida en el marco de la organización correspondiente". [1]

1.1.2. ALCANCE

El alcance de la auditoría define con precisión el entorno y los límites en que va a desarrollarse la auditoría informática y se complementa con los objetivos de ésta. El alcance se concretará expresamente en el informe final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas [26].

1.1.3. TIPOS DE AUDITORÍA INFORMÁTICA

En la Tabla 1.1 se presenta una clasificación de los diferentes tipos de auditorías [4].

Tabla 1.1. Tipos de Auditoría Informática [4]

TIPO	DESCRIPCION
Auditoría de las bases de datos	Controles de acceso, de actualización, de integridad y calidad de los datos.
Auditoría de la seguridad	Referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.
Auditoría de la seguridad lógica	Comprende los métodos de autenticación de los sistemas de información.
Auditoría de la seguridad en producción	Errores, accidentes y fraudes.

Ya que una institución financiera debe garantizar que la información y datos de sus socios sean confidenciales e íntegros, se considera necesario aplicar en el presente trabajo de auditoría los dos primeros tipos mencionados en la Tabla 1.1.

1.1.4. METODOLOGÍAS DE AUDITORÍA INFORMÁTICA

La metodología es necesaria para que un equipo de profesionales alcance un resultado homogéneo tal como si lo hiciera uno sólo. Por ello, resulta habitual el uso de metodologías en las empresas auditoras/consultoras profesionales (desarrolladas por los más expertos) para conseguir resultados similares (homogéneos) en equipos de trabajo diferentes (heterogéneos). [1]

Las metodologías que se puede encontrar en la auditoría informática son dos familias distintas [1]:

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

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

1.1.5. PRINCIPALES PRUEBAS Y HERRAMIENTAS PARA EFECTUAR UNA AUDITORÍA INFORMÁTICA

Al elaborar una auditoría informática el auditor puede realizar las siguientes pruebas [5]:

- **Pruebas clásicas:** Consiste en probar las aplicaciones/sistemas con datos de prueba, observando la entrada, la salida esperada, y la salida obtenida. Existen paquetes que permiten la realización de estas pruebas.
- **Pruebas sustantivas:** Aportan al auditor informático las suficientes evidencias y que se pueda formar un juicio. Se suelen obtener mediante observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones. Verifican así mismo la exactitud, integridad y validez de la información.
- **Pruebas de cumplimiento:** Determinan si un sistema de control interno funciona adecuadamente según la documentación, según declaran los auditados y según las políticas y procedimientos de la organización.

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

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

1.1.6. PROCESO DE UNA AUDITORÍA INFORMÁTICA

El proceso de una auditoría informática se resume en las fases y etapas que se muestran en la Figura 1.1, cuyo detalle se encuentra en el Anexo 1:

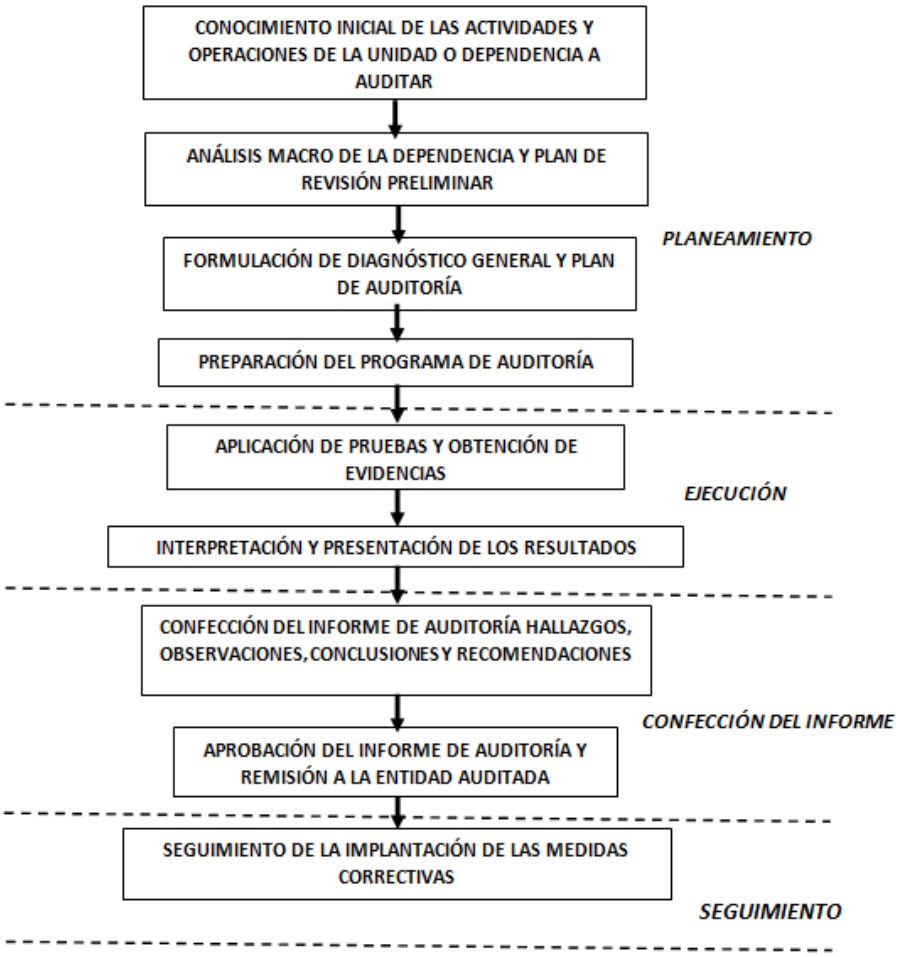


Figura 1.1. Proceso del Operativo de Auditoría[1] .

Todo proceso posee una metodología para ser realizado, es así que el método de trabajo del auditor pasa por las siguientes etapas [18]:

PLANIFICACIÓN DE LA AUDITORÍA INFORMÁTICA

Los ámbitos que deben ser cubiertos dentro de la planificación de la auditoría son:

- Comprensión de la empresa
- Riesgo y materialidad de auditoría
- Objetivos de control y objetivos de auditoría
- Procedimientos de auditoría

1 Fuente: It Governance Institute, Cobit 4.1. (2007), www.itgi.org, http://www.isaca.org/Knowledge-Center/cobit/Documents/cobiT4.1spanish.pdf[44].

EJECUCIÓN DE LA AUDITORÍA INFORMÁTICA

Para el desarrollo adecuado de una auditoría por lo general se debe llevar una apropiada documentación que de modo general incluye:

- Tema de auditoría: Donde se identifica el área a ser auditada.
- Objetivos de auditoría: Donde se indica el propósito del trabajo de auditoría
- Alcances de auditoría: Se detalla los sistemas específicos o unidades de organización que se han de incluir en la revisión en un período de tiempo determinado.
- Planificación previa: Donde se identifica los recursos y destrezas que se necesitan para realizar el trabajo así como las fuentes de información para pruebas o revisión y lugares físicos o instalaciones donde se va auditar.
- Procedimientos de auditoría

FINALIZACIÓN DE LA AUDITORÍA INFORMÁTICA

- Preparación y redacción del informe final
- Redacción de la carta de introducción o carta de presentación del informe final y seguimiento de las medidas correctivas.

1.1.7. ESTÁNDARES DE AUDITORÍA INFORMÁTICA

El auditor de procesos TI tiene una variada gama de herramientas y/o marcos de trabajo que pueden asistirle al momento de aplicar la auditoría que corresponda, dando una visión objetiva para que el auditor decida qué marco es el mejor para usarse en base al medio donde realice su trabajo y dependiendo de la función que cumple la organización: [27].

A continuación en la Tabla 1.2, se resumen en un cuadro comparativo los marcos de trabajo que se han considerado más importantes, cuya principal diferencia entre ellos es el enfoque que manejan para atender y desarrollar las áreas de TI y su cobertura:

Tabla 1.2. Cuadro comparativo entre COBITT, ITIL y la ISO 27000.[2]

ÁREA	COBIT (Gestión de la Seguridad de la Información),	ITIL (Gestión de la Seguridad de la Información)	ISO 27000 (Gestión de la Seguridad de la Información),
Alcance	Abarca todo el espectro de las actividades de IT (seguridad, control,	Muy centrado en la administración de servicios	Cubre todo lo referente a la entrega de servicios de TI

2 Fuentes: http://itilv3-sosw.blogspot.com/2011/05/itil-v3-alineada-con-cobit-41-y-la-iso.html, http://bibdigital.epn.edu.ec/bitstream/15000/2222/1/CD-3019.pdf.

	servicios y riesgo)		
Objetivo principal	Establece controles internos para asegurar buenas prácticas de gestión de IT y un gobierno de IT exitoso.	Dar soporte a los procesos del negocio desde una perspectiva de gestión de servicios.	Definir los requerimientos necesarios para realizar una entrega de servicios de TI alineados con las necesidades del negocio.
Funciones	Mapeo de procesos IT	Mapeo de la Gestión de Niveles de Servicio de IT	Marco de referencia de seguridad de la información
Áreas	4 Procesos y 34 Dominios	9 Procesos	10 Dominios
Creador	ISACA	OGC	ISO International Organization for Standardization
¿Para qué se implementa?	Auditoría de Sistemas de Información	Gestión de Niveles de Servicio	Cumplimiento del estándar de seguridad
¿Quiénes lo evalúan?	Compañías de contabilidad, Compañías de consultoría en TI	Compañías de consultoría en TI	Compañías de consultoría en TI, Empresas de seguridad, Consultores de seguridad en redes.

Además de los estándares de auditoría existen herramientas que ayudan en la auditoría informática, en el presente trabajo se trabajará con el paquete IDEA, el cual permite leer, analizar, visualizar, manipular, obtener muestras y extraer datos de diferentes fuentes, para verificar bases de datos [32].

También se aplicará una herramienta que basada en plugins permite escanear las debilidades de la red, ya sea equipo remoto o equipo local, dicha herramienta es conocida como NESSUS, y se caracteriza por tener alta velocidad de descubrimiento, auditoría en la configuración de aplicaciones y descubrimiento de datos sensibles. [64].

1.2. AUDITORÍA INFORMÁTICA EN EL SECTOR BANCARIO

Esta sección es tomada del libro de Mario Piattini y Emilio del Peso [1] ya que se relaciona con la auditoría informática en el sector financiero, que es el tema principal del proyecto de tesis.

1.2.1. NECESIDAD Y BENEFICIOS DE LA AUDITORÍA INFORMÁTICA EN LAS ENTIDADES FINANCIERAS

Una de las características de cualquier actividad auditora está relacionada con las funciones de control. Por ello la participación de la auditoría informática en el sector financiero la constituye la revisión de las aplicaciones informáticas con el objeto de asegurar que cumplan con los criterios funcionales y operativos definidos por la entidad financiera.

Los sistemas de información de bancos y entidades financieras tienen entre sus características particulares la de construir fuentes de datos para múltiples agentes externos. La importancia de la auditoría informática debe garantizar el correcto funcionamiento de los sistemas, no solo desde la perspectiva de la gestión de la propia empresa sino también desde la óptica de los clientes.

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

1.2.2. AUDITORÍA INFORMÁTICA EN LA PROTECCIÓN DE DATOS PERSONALES

Una entidad financiera dispone de diversa información patrimonial y personal de cada uno de sus clientes. Los datos que posee la entidad pueden ser, sus datos personales (nombre, dirección, teléfono), también puede disponer de datos profesionales (actividad a la que se dedica, empresa para la que trabaja), además posición completa de sus cuentas (saldos), valor tasado de su vivienda en caso de que le haya otorgado un préstamo, nivel de endeudamiento, etc.

La sensibilidad de la información manejada por una entidad financiera es mayor si se tiene en cuenta la totalidad de sus clientes y productos, ya que tienen información más completa y valiosa y por tanto más sensible, que disponer exclusivamente de las cuentas de un único cliente.

Los principales riesgos a los que hace frente la gestión de la información son:

- Difusión no autorizada, intencionada o no, hacia destinos improcedentes. La confidencialidad es un tema de especial preocupación en cualquier entidad financiera ya que en una entidad bancaria interviene la confianza depositada por el cliente.
- Obtención de información errónea, por accidente o por manipulación indebida, y como consecuencia de la normativa a la que está sometida la actividad bancaria perjudicando a los clientes.

1.2.3. ACTIVIDADES DE AUDITORÍA EN RELACIÓN CON LA PROTECCIÓN DE DATOS PERSONALES

Con respecto a la realización de la auditoría, esta debería verificar el cumplimiento de los controles en las áreas siguientes:

- Controles de procedimientos y normas operativas.
- Controles relacionados con la seguridad física.
- Controles relativos a la seguridad lógica.
- Controles de respaldo.

1.3. EJEMPLOS DE APLICACIÓN

1. González Narváez Geovanny y Ruiz Barzola Omar. **Auditoría informática a una institución del sector financiero agencia Guayaquil, período 2008** [20]

"En este trabajo, se realiza la auditoría informática a una sucursal bancaria en un periodo determinado aplicando técnicas de auditoría básicas para determinar la integridad, disponibilidad y confidencialidad de la información".

El estudio comprende desde un conocimiento completo de la institución hasta la emisión de un informe de las observaciones encontradas con sus respectivas recomendaciones.

Adicionalmente desarrollan un pequeño análisis estadístico, el cual comprende determinar el grado de satisfacción de los usuarios actuales hacia el sistema que utilizan, y la importancia y grado de aceptación que se tiene en migrar los datos a un nuevo sistema.

Además pudieron constatar que la institución carece de seguridades físicas y lógicas en el manejo de la información de todos sus departamentos debido a los sistemas caducos que posee.

Entre las recomendaciones del presente trabajo presentan las siguientes:

- Establecer y hacer cumplir políticas para tener un mayor control con los servidores donde se especifique mantener la sesión de usuario cerrada.
- Elaborar aplicativos del sistema que elaboren procesos automáticamente.
- Designar un equipo de evaluación de sistemas para que mitigue errores potenciales.
- Escoger un lugar apropiado y seguro para los respaldos diarios de todas las áreas.
- Eliminar ciertos atributos que poseen los usuarios para evitar que se acceda a módulos o áreas críticas que pueden ocasionar que la información deje de ser integra.

Con esta investigación logran conocer la situación real en la que se encuentra la agencia de Guayaquil de la entidad financiera auditada, con respecto a la tecnología de la información.

2. Carlos Geovanny Guzmán de León. **Lineamientos Generales para una Auditoría de Sistemas en el Centro de Información de una Institución Bancaria** [24].

"Este trabajo fue realizado tomando en cuenta la importancia que tiene la función de la auditoría de sistemas en las instituciones financieras, así como la necesidad de planificarla o desarrollarla"

En esta investigación determinan las estrategias y cursos de acción de la institución financiera, las cuales se establecen mediante entrevistas y un análisis detallado de cada proceso básico de la organización.

Éste estudio contempla, a manera general, las siguientes características:

- Un proceso que involucra todas las áreas de la institución financiera
- Evalúan el medio externo en sus diferentes entornos
- Se apoya en asesores externos o especialistas de la institución financiera
- Detecta fortalezas, debilidades y áreas de oportunidad de la institución financiera (financieras, recursos humanos, tecnología, mercadotecnia, etc.)
- Establecen las amenazas que representa la competencia
- Determinan estrategias y metas de la institución financiera
- Los proyectos se contemplan a corto, mediano y largo plazo
- Aprobación del informe de auditoría, por los accionistas o dueños de la institución financiera

Para el desarrollo de la auditoría de sistemas realizan un muestreo en el sector financiero del país (instituciones bancarias), debido a la gran cantidad de datos que manejan, el tipo de operaciones (puntos de venta, cajeros automáticos, agencias y otros), y el personal que existe en sus centros de información.

En este proyecto hablan del marco de trabajo COBIT para el desarrollo e implantación de la auditoría informática, pero no detallan la aplicación del mismo en el desarrollo de la investigación.

Entres las recomendaciones que se emiten en este proyecto tenemos que:

- Las instituciones financieras deben crear un plan estratégico de acuerdo a los objetivos de la organización en donde se desempeñan, para poder obtener mejores frutos.
- Los escasos auditores de sistemas que se encuentran en nuestro medio deben capacitarse con personal calificado, en las distintas aéreas de dicha auditoría, lo que les proporcionará las herramientas y el conocimiento necesarios para garantizar plena confianza en la exactitud e integridad de los datos que son generados por los sistemas de información.
- Tomar en cuenta por parte de la administración (Junta Directiva y/o Presidencia) de cada una de las instituciones financieras, el adelanto tecnológico del que son objeto los sistemas de información.
- Adoptar una metodología de acuerdo a los estándares de calidad ISO, para poder llevar a cabo de una manera organizada las auditorías en los centros de información.

- Brindar a los miembros de la unidad de auditoría de sistemas, una capacitación constante de acuerdo a las necesidades del centro de información y a las necesidades tecnológicas de nuestro medio.

3. Fayer Alexis Calderón Yong. **Auditoría Informática Aplicando COBIT 4.0 en la Cooperativa de Ahorro y Crédito "Pablo Muñoz Vega" Ltda.** [11].

"Este trabajo realiza un análisis de riesgos en conjunto con los procesos del marco de trabajo COBIT 4.0 para poder determinar en qué nivel de riesgo tecnológico se encuentra el área de sistemas y por ende la Cooperativa de Ahorro y Crédito "Pablo Muñoz Vega Cia. Ltda". Luego efectúa un análisis de cada proceso de COBIT para poder determinar las fortalezas y debilidades tecnológicas de la institución, planteando finalmente la aplicación de mejoras o correctivos necesarios para monitorear y controlar el área de TI".

El principal objetivo de esta auditoría informática es asesorar a la administración de la cooperativa en el cumplimiento efectivo de sus responsabilidades, facilitándoles análisis, apreciaciones, comentarios y recomendaciones relacionados con las actividades del procesamiento de la información.

Con el desarrollo de la auditoría informática se pretende, evaluar lo correspondiente a la tecnología de la información de la cooperativa y lograr con ello un adecuado retorno de la inversión que se realza en tecnología, que la institución posea una correcta administración de los riesgos en TI, y que disponga de un apropiado marco de control interno.
Para cumplir con el objetivo de la auditoría se recabó toda documentación e información correspondiente al área de sistemas de la cooperativa acorde a cada proceso de COBIT 4.0.

Para ello, en primer lugar realizan un análisis de riesgo a nivel tecnológico, con cual tienen una visión general de posibles riesgos en cuanto a tecnología que podrían presentarse en la Cooperativa de Ahorro y Crédito "Pablo Muñoz Vega" Ltda. Posteriormente aplicando el modelo de madurez de cada una de los procesos de COBIT 4.0 presenta el informe final de la auditoría informática, el que permitirá a la cooperativa tener una apreciación de cómo y en qué estado se encuentra su área de sistemas, emitiéndose en este informe las observaciones vertidas por cada uno de dichos procesos.

Entres las recomendaciones que se emiten en este proyecto tenemos que:

- Se considera importante que el personal tanto del área de sistemas como de auditoría interna, unidad de riesgos y la alta dirección reciban una inducción en la metodología de auditoría para que su aplicación sea más productiva y los resultados de la evaluación sean elementos de juicio para toma de decisiones.
- Basados en los lineamientos de la metodología COBIT para el área de TI, las organizaciones deben adoptar las mejores prácticas y adaptarlas a sus procesos para alcanzar un nivel óptimo de madurez para mejorar la competitividad de la organización.
- Diseñar un proceso de implementación de las recomendaciones generadas en la evaluación de auditoría efectuada, el mismo que complementaría el objetivo principal de la ejecución de la auditoría informática que consiste en la mejora continua de los procesos de TI.

1.4. COBIT COMO MARCO DE REFERENCIA PARA AUDITORÍA INFORMÁTICA

1.4.1. ESTRUCTURA DEL MARCO REFERENCIAL COBIT

El marco de referencia de COBIT consta de objetivos de control de TI de alto nivel y de una estructura general para su clasificación y presentación, que han sido basadas en tres niveles de actividades de TI al considerar la administración de sus recursos, estos son [2]:

- **Actividades:** las actividades y tareas son las acciones requeridas para lograr un resultado medible. Las actividades tienen un ciclo de vida, mientras que las tareas son más discretas.
- **Procesos:** son conjuntos de actividades o tareas con delimitación o cortes de control.
- **Dominios:** es la agrupación natural de procesos denominados frecuentemente como dominios que corresponden a la responsabilidad organizacional.

Por lo tanto, el marco de referencia conceptual puede ser enfocado desde tres puntos estratégicos: criterios de información, recursos de TI y procesos de TI.

Estos tres puntos estratégicos son descritos en el cubo COBIT que se ilustra en Figura 1.2.

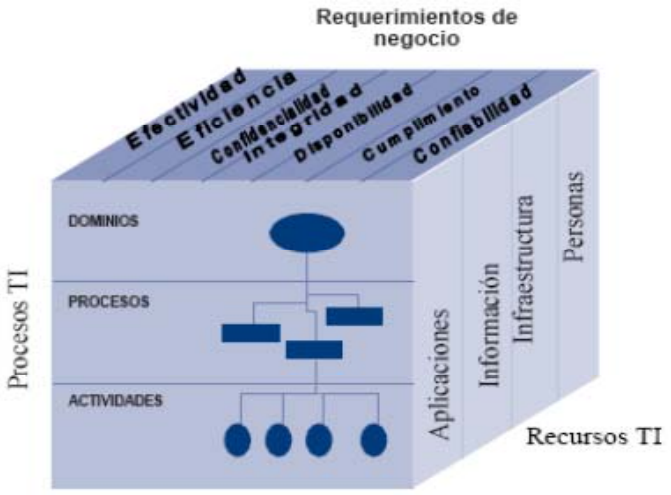


Figura 1.2. Cubo COBIT[3]

Para lograr la alineación de las mejores prácticas con los requerimientos del negocio, se recomienda que COBIT se utilice al más alto nivel, brindando así un marco de control general basado en un modelo de procesos de TI que debe ser aplicable en general a toda empresa.

[3] Fuente: It Governance Institute, *Cobit 4.1.* (2007), www.itgi.org, http://www.isaca.org/Knowledge-Center/cobit/Documents/cobiT4.1spanish.pdf [2].

1.4.2. DOMINIOS

COBIT presenta treinta y cuatro objetivos generales, uno para cada uno de los procesos de las TI, estos procesos están agrupados en cuatro dominios como lo muestra la Figura 1.3:

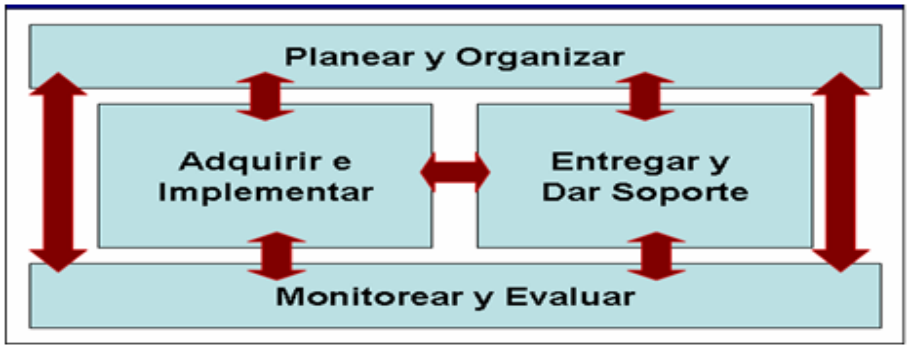


Figura 1.3. Los cuatro dominios de COBIT [4]

1.4.2.1. PLANEAR Y ORGANIZAR (PO)

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada [2].

Este dominio considera los siguientes objetivos de alto nivel o procesos:

- PO1 Definir un plan estratégico de tecnología de información
- PO2 Definir la arquitectura de Información
- PO3 Determinar la dirección tecnológica
- PO4 Definir la organización y de las relaciones de TI
- PO5 Manejar la inversión en Tecnología de Información
- PO6 Comunicar la dirección y aspiraciones de la gerencia
- PO7 Administrar recursos humanos
- PO8 Asegurar el cumplimiento de requerimientos externos
- PO9 Evaluar riesgos
- PO10 Administrar proyectos
- PO11 Administrar calidad

[4] Fuente: It Governance Institute, *Cobit 4.1.* (2007), www.itgi.org, http://www.isaca.org/Knowledge-Center/cobit/Documents/cobiT4.1spanish.pdf [4].

1.4.2.2. ADQUIRIR E IMPLEMENTAR (AI)

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como la implementación e integración en los procesos del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes [2].

Este dominio considera los siguientes objetivos de alto nivel o procesos:

- AI1 Identificar soluciones
- AI2 Adquirir y mantener software de aplicación
- AI3 Adquirir y mantener arquitectura de tecnología
- AI4 Desarrollar y mantener procedimientos relacionados con TI
- AI5 Instalar y acreditar sistemas
- AI6 Administrar cambios

1.4.2.3. ENTREGAR Y DAR SOPORTE (DS)

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales [2].

Este dominio considera los siguientes objetivos de alto nivel o procesos:

- DS1 Definir niveles de servicio
- DS2 Administrar servicios prestados por terceros
- DS3 Administrar desempeño y capacidad
- DS4 Asegurar servicio continuo
- DS5 Garantizar la seguridad de sistemas
- DS6 Identificar y asignar costos
- DS7 Educar y entrenar a los usuarios
- DS8 Apoyar y asistir a los clientes de TI
- DS9 Administrar la configuración
- DS10 Administrar problemas e incidentes
- DS11 Administrar datos
- DS12 Administrar instalaciones
- DS13 Administrar operaciones

1.4.2.4. MONITOREAR Y EVALUAR (ME)

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del

desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno [2].

Este dominio considera los siguientes objetivos de alto nivel o procesos:

- M1 Monitorear los procesos
- M2 Evaluar lo adecuado del control Interno
- M3 Obtener aseguramiento independiente
- M4 Proporcionar auditoría independiente.

En resumen, los Recursos de TI necesitan ser administrados por un conjunto de procesos agrupados en forma natural, con el fin de proporcionar la información que la empresa necesita para alcanzar sus objetivos [14].

COBIT es considerada una herramienta completa ya que permite administrar los sistemas de información a un nivel más alto que los estándares existentes para el mismo propósito.

Se ha determinado que por las características y ambiente de aplicación de COBIT, ésta es la herramienta más útil para fundamentar el presente proyecto, ya que, independientemente de la misión de la organización a ser auditada, la plataforma en la que se basa el desarrollo de las tecnologías de la información, el servicio o producto que ofrezca, el tipo de administración que predomine; el marco de referencia COBIT no es sólo una guía para auditores o técnicos profesionales en procesos TI, sino también para gerentes y todos quienes están involucrados en el cumplimiento de los objetivos del negocio, pues en ambos aspectos, gerencial y tecnológico, su implementación será fundamental para que el gobierno de TI se desarrolle como debe ser.

1.4.3. OBJETIVOS DE CONTROL

Un objetivo de control de TI es una declaración del resultado o fin que se desea lograr al implantar procedimientos de control en una actividad de TI en particular. Los objetivos de control de COBIT son los requerimientos mínimos para un control efectivo de cada proceso de IT. Ya que los objetivos de control de TI de COBIT están organizados por procesos de TI, el marco de trabajo brinda vínculos claros entre los requerimientos de gobierno de TI, los procesos de TI y los controles de TI [2].

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 [2].

Los objetivos de control detallados se identifican por dos caracteres que representan el dominio (PO, AI, DS y ME) más un número de proceso y un número de objetivo de control [2].

Además de los objetivos de control detallados, cada proceso COBIT tiene requerimientos de control genéricos que se identifican con PCn (Control de Proceso número). Estos se deben tomar como un todo junto con los objetivos de control del proceso para tener una visión completa de los requerimientos de control [2], los cual se detalla en el Anexo 2.

COBIT también ofrece un conjunto recomendado de objetivos de control de las aplicaciones identificados por ACn, número de Control de Aplicación [2], esto también se explica detenidamente en el Anexo 2.
Una descripción detallada de cada proceso COBIT con su respectivo objetivo de control se puede encontrar en el Anexo 16.

1.4.4. MODELOS DE MADUREZ

Los modelos de madurez para el control de los procesos de TI consisten en desarrollar un método de puntaje de modo que una organización pueda calificarse a sí misma desde inexistente hasta optimizada (de 0 a 5). Este método ha sido derivado del modelo de madurez que el Software Engineering Institute definió para la madurez de la capacidad de desarrollo de software. Contra estos niveles, desarrollados para cada uno de los treinta y cuatro procesos de TI de COBIT, la administración puede mapear o cruzar [2]:

- El estado actual de la organización - dónde está la organización actualmente
- El estado actual de la industria (la mejor de su clase en) - la comparación
- El estado actual de los estándares internacionales - comparación adicional
- La estrategia de la organización para mejoramiento - dónde quiere estar la organización.

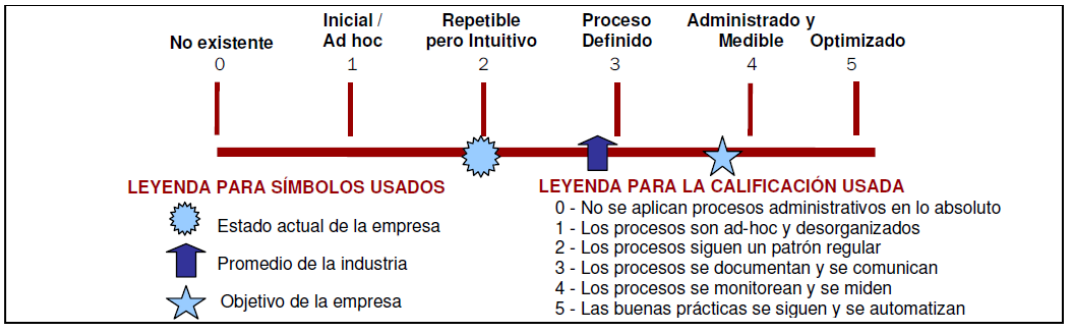


Figura 1.4. Representación gráfica de los modelos de madurez[5]

0 Inexistente. Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.

[5] Fuente: It Governance Institute, *Cobit 4.1.* (2007), www.itgi.org, http://www.isaca.org/Knowledge-Center/cobit/Documents/cobiT4.1spanish.pdf [2].

1 Inicial. Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.
2 Repetible. Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.
3 Definido. Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.
4 Administrado. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.
5 Optimizado. Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

En resumen, los modelos de madurez brindan un perfil genérico de las etapas a través de las cuales evolucionan las empresas para la administración y el control de los procesos de TI, este perfil es [2]:

- Un conjunto de requerimientos y los aspectos que los hacen posibles en los distintos niveles de madurez
- Una escala donde la diferencia se puede medir de forma sencilla
- Una escala que se presta a sí misma para una comparación práctica
- La base para establecer el estado actual y el estado deseado
- Soporte para un análisis de brechas para determinar qué se requiere hacer para alcanzar el nivel seleccionado
- Tomado en conjunto, una vista de cómo se administra la TI en la empresa.

CAPÍTULO 2:

ANÁLISIS SITUACIONAL DE LA COOPERATIVA DE AHORRO Y CRÉDITO "FORTUNA"

2. *ANÁLISIS SITUACIONAL DE LA COOPERATIVA DE AHORRO Y CRÉDITO "FORTUNA"*

Durante el desarrollo de esta fase se conocerá más a fondo a la Cooperativa de Ahorro y Crédito "Fortuna", realizando el análisis situacional de la misma, esto es, su descripción, su infraestructura, cómo está organizada estructuralmente, cómo está conformada su área de sistemas, cómo está estructurada físicamente, qué sistema se utiliza y sobre qué base de datos trabaja, cuál es su plataforma de desarrollo, productos y servicios que ofrece, entre otros temas; dándonos con ello una idea general de la misma, pues es la empresa en la cual se desarrolla el presen te trabajo de tesis.

Con estos conocimientos previos se define la problemática, se establece el plan de auditoría informática, el cual contempla el objetivo principal, el alcance de la auditoría, quién va realizar la auditoría, qué personas estarán involucradas y el proceso que se sigue para otorgar un crédito en la cooperativa "Fortuna".

Además se definen los procesos de crédito que se realizan en la cooperativa para la otorgación de créditos a sus socios, mismos que se encuentran esquematizados en un gráfico, posteriormente se realiza la elección de los procesos correspondientes a los dominios del marco referencial COBIT, estos han sido seleccionados en base al criterio del auditor, haciendo relación con el proceso de crédito que se realiza en la cooperativa, mismo que se ha seleccionado para realizar la auditoría informática.

2.1. DEFINICIÓN DE LA PROBLEMÁTICA

La Cooperativa de Ahorro y Crédito "Fortuna" dentro del proceso de planificación y mejoramiento de la calidad de sus servicios ha tomado como un hito principal realizar un adecuado seguimiento y control de los procesos de negocio, principalmente en el departamento de crédito y de TI que son la columna vertebral de toda institución financiera.

Es por ello que se ha establecido como proceso inicial la realización de una auditoría informática a dichos procesos, tomando como marco de trabajo a COBIT, para de esta manera verificar el cumplimiento de las normativas de la cooperativa dentro del proceso crediticio, y a partir de este estudio encontrar las diferentes falencias y proponer posibles mejoras que puedan adoptarse en la institución, tanto en el área de crédito como en el área de tecnología de información; y de la misma manera, asegurar que el sistema informático cumpla con los requerimientos de la entidad, permitiendo un adecuado manejo y control de los procesos de crédito.

2.2. ANTECEDENTES

La Cooperativa de Ahorro y Crédito "Fortuna" funciona en la ciudad de Loja desde hace siete años y es una institución financiera que trabaja al servicio de todos sus socios.

El sistema que utiliza la Cooperativa de Ahorro y Crédito "Fortuna" tiene por nombre "CONEXUS" el cual posee módulos operativos, módulos administrativos, módulos de control, módulos adicionales e interfaces externas, los cuales se detallan en el Anexo 3 . Este sistema es centralizado ya que se encuentra localizado en el servidor LINUX, y por ende todas las terminales acceden a éste para cualquier operación que se desee efectuar.

La cooperativa posee dos servidores, uno para la base de datos el cual trabaja con el sistema operativo LINUX CENTOS 5.2., y cuyo motor de base de datos es INFORMIX instalado sobre un servidor hp con tecnología INTEL XEON, Y el segundo bajo la plataforma de Windows 2000 Service Pack 4 que controla bajo un software propio del sistema "CONEXUS" los usuarios logueados al mismo (control de licencias por usuarios) y está desarrollado en Visual Basic 6.0.

La página web de la Cooperativa de Ahorro y Crédito "Fortuna" [22] contiene toda la información correspondiente a ella, en lo que respecta a su misión, visión, productos financieros, servicios e información financiera. Siendo ésta una página estática ya que se encuentra en proyecto la elaboración de una página web dinámica con más servicios para todos sus socios.

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

Las personas involucradas en el desarrollo de esta auditoría son:

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

Este trabajo de auditoría informática servirá como una herramienta, tanto para el departamento de crédito, como para el departamento de auditoría interna de la cooperativa "Fortuna", el cual permitirá efectuar evaluaciones periódicas al área de crédito, área de sistemas y al aplicativo "CONEXUS".

2.3. INFORMACIÓN INSTITUCIONAL

2.3.1. DESCRIPCIÓN DE LA EMPRESA

La Cooperativa de Ahorro y Crédito "Fortuna", se crea el 27 de Noviembre del 2003, con treinta y nueve socios fundadores, en su mayoría Lojanos.

Esta prestigiosa institución, se inscribió legalmente en el Registro General de Cooperativas con el número de orden 6630, y se registraron sus estatutos en el Registro Mercantil del Cantón Loja del año 2006, bajo partida N.-105, y anotado en el repertorio con el N.-1195.

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

2.3.2. MISIÓN

Brindar a sus socios y comunidad lojana el mejor servicio cooperativo, competitivo y oportuno para contribuir al desarrollo económico y social de cada uno de los sectores de su economía, incentivando el ahorro y el crecimiento mutuo.

2.3.3. VISIÓN

Ser la cooperativa de ahorro y crédito líder en la ciudad y provincia de Loja, mediante la prestación de productos y servicios financieros de calidad, conforme a los requerimientos de sus socios y ciudadanía en general con solvencia, agilidad y honradez, garantizando de esta manera la seguridad de sus depósitos y siendo una mano amiga a la hora de necesitar su apoyo.

2.3.4. VALORES

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

2.3.5. OBJETIVOS INSTITUCIONALES

Objetivos generales

- Fortalecer el patrimonio institucional.
- Integrar a los socios con la institución.
- Mejorar la atención al socio y cliente.

Objetivos específicos

- Obtener un crecimiento sostenido y transparente de activos y pasivos.
- Realizar el manejo eficiente de la cartera de crédito y su morosidad.

- Mantener costos de operación mínimos.
- Adquirir la tecnología adecuada para servir mejor al socio, así como para contrarrestar el riesgo operativo.
- Ofrecer a nuestros socios y ciudadanía en general calidad en los productos y servicios con bajos costos para obtener ventaja competitiva.
- Crear productos innovadores acorde con los requerimientos de nuestros socios y ciudadanía en general.
- Mejorar el ambiente laboral, donde el personal desenvuelva sus capacidades de manera eficiente.
- Implementar un plan de capacitación continua al personal de la institución con el fin de alcanzar objetivos en común con la cooperativa.
- Establecer normas que permitan reducir gastos para tener mejores resultados al final de cada periodo.
- Elaborar un plan de publicidad dirigido a todos los socios para mantener al socio informado de los nuevos servicios y beneficios que ofrece la cooperativa.
- Realizar el presupuesto estructurado para la construcción del edificio casa matriz de la cooperativa, aprovechando que se cuenta con el terreno ubicado en el centro de la ciudad.
- Realizar el control periódico del desempeño de los concejos y comisiones de la cooperativa con el fin de que cumplan sus funciones de manera eficiente.
- Implementar una red de cajeros automáticos en las instalaciones de la cooperativa.
- Desarrollar el plan de contingencias para la recuperación de información en caso de desastres informáticos con el fin de eliminar el riesgo operativo.

2.3.6. PRODUCTOS Y SERVICIOS

- **Ahorros**
  Son los depósitos a la vista que efectúan los socios a los cuales se les paga una tasa de interés acorde al mercado, sobre el saldo que mantenga en su libreta.
- **Ahorro Estudio, Ahorro Navidad, Ahorro Vacaciones, Ahorro Fondos de Reserva**
  Es un ahorro programado cooperativo al cual se le paga una de interés preferencial siempre que se encuentre dentro del mercado, los depósitos que realizan en éste producto son mensuales y se pueden disponer de ellos al año de aportaciones.
- **Depósitos a Plazo Fijo**
  Son los depósitos a corto y mediano plazo, que realizan socios y clientes, a los cuales se les paga una tasa de interés acorde al mercado.
- **Créditos**
  La cooperativa ofrece una variedad de créditos a sus socios, así como: créditos de consumo, comercio, microcrédito y vivienda, con garantías personales, garantía hipotecaria y garantía prendaria y garantía de aval.

- **Garantías cooperativas**
  Es un aval que la cooperativa emite a favor de los profesionales de la construcción, para garantizar el trabajo que desarrollen con instituciones públicas o privadas.
- **Pago de remuneraciones**
  La cooperativa puede cancelar los sueldos al personal de las instituciones que desee cobrarlo, a través de un convenio con las asociaciones.
- **Seguro de vida y accidentes**
  El afiliado que mantenga su cuenta activa tiene el beneficio de una cobertura de seguro de vida y accidentes en los casos de muerte natural y muerte accidental, y gastos de sepelio, atención médica gratuita, descuentos especiales en asistencia oftalmológica, odontología y compra de medicina
- **Pago de servicios básicos**
  La cooperativa ofrece a sus socios el pago de servicios a través de las libretas de ahorros, con los descuentos por el consumo que realizan tanto de luz, teléfono, agua potable.

2.3.7. INFRAESTRUCTURA

Actualmente la cooperativa tiene una oficina matriz ubicada en la ciudad de Loja, en las calles Bolívar entre Quito e Imbabura, sin sucursales a la fecha.

2.3.8. ORGANIGRAMA ESTRUCTURAL

La Cooperativa de Ahorro y Crédito "Fortuna" se encuentra estructurada según lo muestra la Figura 2.1.

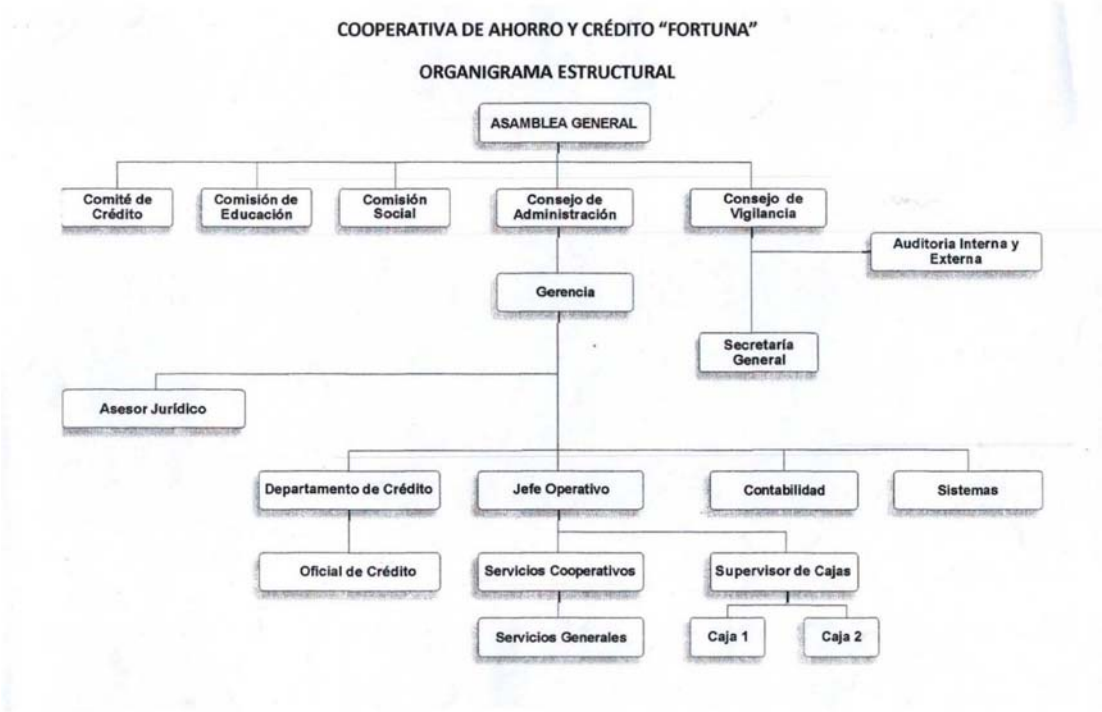


Figura 2.1. Organigrama Estructural de la Cooperativa de Ahorro y Crédito "Fortuna".

2.3.8.1. DEPARTAMENTO DE SISTEMAS

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

- Jefe de sistemas
- Operador de sistemas y soporte al usuario

Actualmente el departamento de sistemas no tiene elaborado su organigrama.

2.3.8.2. DEPARTAMENTO DE CRÉDITO

El departamento de crédito de la Cooperativa de Ahorro y Crédito "Fortuna" se encuentra conformado por las siguientes personas:

- Oficial de crédito 1
- Oficial de crédito 2
- Asesor legal

Esto se ve reflejado en la Figura 2.1.

Existen algunas falencias en este departamento tanto operativas como automatizadas, las cuales serán evaluadas en este estudio.

2.4. ESTRATEGIA GENERAL

2.4.1. ANTECEDENTES

Con la finalidad de evaluar el control de los procesos críticos de crédito de la Cooperativa de Ahorro y Crédito "Fortuna", se ha visto en la necesidad de realizar una auditoría informática, utilizando como base de evaluación el marco referencial COBIT.

2.4.2. ALCANCE

El alcance de la presente evaluación está determinada por los procesos de los cuatro dominios como son: Planificar y organizar, adquirir e implementar, entregar y dar soporte, monitorear y evaluar, del marco referencial COBIT en el ámbito de los procesos Crédito y de TI de La Cooperativa de Ahorro y Crédito "Fortuna".

2.4.3. EQUIPO AUDITOR

Karolay Michell Coronel Castro.

2.4.4. INVOLUCRADOS

- Gerente general
- Personal de sistemas
- Personal de crédito
- Director/Co-directora de tesis

2.5. PROCESOS DE CRÉDITO EN LA COOPERATIVA "FORTUNA"

En esta sección se detallan los procesos que se realizan en la Cooperativa de Ahorro y Crédito "Fortuna", se hace una selección de los procesos a auditar en base a una matriz de probabilidad de ocurrencia de un proceso de crédito y también se elaboran diagramas SIPOC los cuales esquematizan los procesos seleccionados para auditar.

Existen varios procesos que se realizan el departamento de crédito de la cooperativa, los cuales se listan a continuación:

- Análisis del crédito
- Aprobación del crédito

- Legalización del crédito
- Desembolso del crédito
- Recuperación del crédito.
- Constitución de hipotecas y prendas
- Levantamiento de hipotecas y prendas
- Compra de documentos
- Castigo de créditos

La Tabla 2.1 muestra la matriz de probabilidad de ocurrencia de un proceso de crédito, en la cual de acuerdo a determinados criterios se establece la posibilidad de que se de un proceso, al cual se le asigna una calificación de uno a cuatro, siendo cuatro la calificación más alta.

Tabla 2.1. Matriz de Probabilidad de Ocurrencia de un Proceso de Crédito .

MATRIZ DE PROBABILIDAD DE OCURRENCIA DE UN PROCESO DE CRÉDITO		
PROBABILIDAD	**CRITERIO**	**CALIFICACIÓN**
Muy probable	El proceso ocurre a diario	4
Probable	El proceso ocurre semanalmente	3
Posible	El proceso ocurre mensualmente	2
Poco probable	El proceso ocurre anualmente	1

La Tabla 2.2 muestra la selección de los procesos de crédito a auditarse, en base a los criterios establecidos en la Tabla 2.1, los procesos con calificación cuatro y tres han sido determinados como los procesos cotidianos, por lo que son más susceptibles a errores, por lo tanto deben ser analizados.

Tabla 2.2. Procesos de Crédito a Auditar.

PROCESO	SE AUDITA?
Análisis del crédito	✓
Aprobación del crédito	✓
Legalización del crédito	✓
Desembolso del crédito	✓

Recuperación del crédito	✓
Constitución de hipotecas y prendas	-
Levantamiento de hipotecas y prendas	-
Compra de documentos	-
Castigo de créditos	-

Con la correspondiente matriz de evaluación de ocurrencia, se determinó que de nueve procesos de crédito que se llevan a cabo en el departamento de crédito de la cooperativa, cinco requieren ser auditados.

A continuación se detallan los procesos a auditarse y sus respectivos diagramas SIPOC.

2.5.1. PROCESOS PARA OTORGAR CRÉDITOS A LOS SOCIOS

2.5.1.1. PRIMER PROCESO (PC1): ANÁLISIS DEL CRÉDITO

Objetivo del Proceso: Revisión y análisis de la documentación presentada por el socio, y elaboración del informe de crédito por parte del oficial, el mismo que es remitido al comité de crédito.

Detalle del Proceso:

- **Revisión de documentación:**

  El oficial de crédito revisa la documentación presentada por el socio, esto incluye que la solicitud de crédito y el estado económico del garante estén llenos con los respectivos datos que se piden y que estén debidamente firmados, además de que los requisitos solicitados estén completos.

  El crédito puede ser solicitado bajo garantes, bajo garantía hipotecaria, garantía prendaria, garantía de un aval, con garante hipotecario, garante prendario o garante con aval, este tipo de garantía depende de cómo lo quiera hacer el socio y también depende del monto que solicite.

  Se revisa el buró de crédito (central de riegos) del solicitante y garantes si es el caso de un crédito con garantes.

  Se confirman que las direcciones domiciliarias y certificados de trabajo del solicitante y garantes sean verídicos.

- **Estudio de la situación financiera del solicitante:**
  Se analiza la situación económica del solicitante y garantes en base a los ingresos justificados, a los gastos declarados en la respectiva solicitud de crédito y estado económico, y al reporte del buró de crédito.
- **Elaboración del informe de crédito:**
  Se elabora el medio de aprobación (informe de crédito, Anexo 4) en el cual se resume toda la información del crédito, del socio y su garantía.
  Toda la documentación se archiva en una carpeta para ser entregada al comité de crédito.

Diagrama SIPOC del Proceso:

A continuación se emite una descripción previa al diagrama de la Figura 2.2, para una mejor comprensión del mismo.

Proveedores:

Socio: Cuenta ahorrista de la cooperativa.

Garantía: Respaldo del crédito, puede ser del tipo personal (garantes) respaldada por las firmas de los mismos, del tipo hipotecaria con respaldo de un bien inmueble, del tipo prendaria con respaldado de un vehículo o maquinaria, del tipo aval con respaldo de un certificado de depósito a plazo, generado por la cooperativa (Anexo 26), las garantías también pueden ser por medio de un garante hipotecario, garante prendario o garante con aval.

Tipo de garantía hipotecaria: Está formada por las escrituras del bien a hipotecar, un certificado historiado del bien a hipotecar y el avaluó del bien a hipotecar, el cual es informe detallado y con valor del bien inmueble que respaldará el crédito, este avaluó es realizado por el perito avaluador de la cooperativa.

Tipo de garantía prendaria: Está formada por la copia de la matrícula del vehículo o maquinaria, y el avaluó del mismo, el cual es un informe detallado y con valor del vehículo o maquinaria que respaldará el crédito, este es realizado por el perito avaluador de la cooperativa.

Garante hipotecario: Persona que respalda el crédito con su bien inmueble y con su firma.

Garante prendario: Persona que respalda el crédito con su vehículo o prenda y con su firma.

Garante con aval: Persona que respalda el crédito con su certificado de depósito de ahorro a plazo y con su firma.

Certificado de depósito de ahorro a plazo: póliza a plazo fijo (Anexo 26)

Buró de crédito: empresa constituida como sociedad de información crediticia, que proporciona información, previo a la concesión de un crédito, cuyo objetivo principal es registrar el historial crediticio de las personas y empresas que hayan obtenido algún tipo de crédito, financiamiento, préstamo o servicio, a este servicio se tiene acceso por medio de una página web

Sistema: Software financiero utilizado en la Cooperativa de Ahorro y Crédito "Fortuna" el cual lleva el nombre de "CONEXUS".

Entradas:

Solicitud de crédito: documento impreso que recaba toda la información personal y económica del solicitante del crédito (Anexo25)

Documentación personal: copias de cédulas y de certificados de votación.

Documentación de ingresos: certificado de trabajo/rol de pagos/ruc y declaraciones al SRI.

Documentación de patrimonio: predios de bienes inmuebles y copias de matrículas de vehículos o maquinaria.

Estado económico: documento impreso que recaba toda la información personal y económica del garante del crédito (Anexo 31).

Historial crediticio: Reporte obtenido del buró de crédito, en el que se detallan el endeudamiento de una persona, así como su historial de pagos (Anexo 24).

Reporte de estado económico del socio: Reporte que emite el sistema y que detalla la información de los saldos de la cuenta del socio, así como información de créditos o garantías vigentes en la cooperativa, e información de inversiones con certificados de depósito a plazo en la cooperativa (Anexo 30).

Salidas:

Medio de aprobación: informe de crédito en formato Excel el cual posee un resumen de todos los datos concernientes al crédito (Anexo 4).

Clientes:

Comité de crédito: Gerente y socios fundadores de la cooperativa elegidos para la revisión de las solicitudes de crédito.

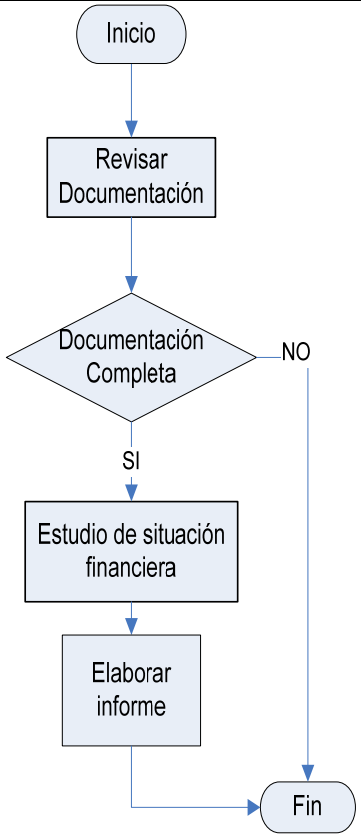
PROVEEDORES	ENTRADAS	PROCESO	SALIDA	CLIENTES
Socio Garantía Buró de Crédito Sistema "CONEXUS"	Solicitud de crédito Documentación personal Documentación de ingresos Documentación de patrimonio Hoja de estado económico Documentación personal Documentación de ingresos Documentación de patrimonio Historial crediticio Reporte de estado económico del socio.		Medio de aprobación	Comité de Crédito

Figura 2.2. Diagrama SIPOC del proceso de Análisis del Crédito.

2.5.1.2. SEGUNDO PROCESO (PC2): APROBACIÓN DEL CRÉDITO

Objetivo del Proceso: Revisión, análisis y veredicto del comité de crédito.

Detalle del Proceso:

- **Exposición del crédito :**

  Dependiendo el monto que solicite el socio, la gerente o el oficial de crédito exponen el informe del crédito al comité, dando lectura al medio de aprobación y mostrando toda la documentación presentada por el socio.

  Si la solicitud de crédito es de hasta $2000.00, es aprobada únicamente por la gerencia.

  Si la solicitud de crédito es desde $2001.00 hasta $7500.00, es aprobada por el comité de crédito el cual está formado por dos socios fundadores de la cooperativa y la gerente.

Si la solicitud de crédito es desde $7501.00 hasta el 10% del patrimonio actual de la cooperativa, es aprobada por el Consejo de Administración el cual está formado por cinco socios fundadores de la entidad.

- **Análisis del crédito:**
  El comité encargado de aprobar la solicitud presentada, analiza la petición, documentación y el medio de aprobación y emite su resolución.
- **Resultados obtenidos:**
  En caso de ser aprobada la petición de crédito se firma la aprobación en la solitud de crédito presentada por el socio, esta aprobación queda sentada en las actas de crédito (Anexo 12).
  Si el crédito fue negado, no se firma la solicitud de crédito y se devuelve la carpeta del socio al oficial de crédito para que esta sea entregada al socio previa explicación de por qué motivo se tomó esta resolución.

Diagrama SIPOC del Proceso:

A continuación se emite una descripción previa al diagrama de la Figura 2.3 para una mejor comprensión del mismo.

Proveedores:

Oficial de crédito: Funcionario de la cooperativa encargada de ayudar a los socios o empresas para obtener los créditos.

Gerente: Persona que está a cargo de la dirección de la cooperativa.

Comité de crédito: Socios fundadores de la cooperativa, asignados para revisar las solicitudes de crédito.

Entradas:

Carpeta del socio: Folder con toda la documentación presentada por el socio y toda la información que adiciona el oficial de crédito cuando hace el análisis del crédito**.**

Firmas en solicitud de petición del crédito: Firmas con las que los miembros del comité de crédito aceptan la aprobación del crédito solicitado.

Salidas:

Crédito aprobado o negado: Respuesta a la petición del crédito.

Clientes:

Socio: Cuenta ahorrista de la cooperativa.

Oficial de crédito: Funcionario de la cooperativa encargada de ayudar a los socios o empresas para obtener los créditos.

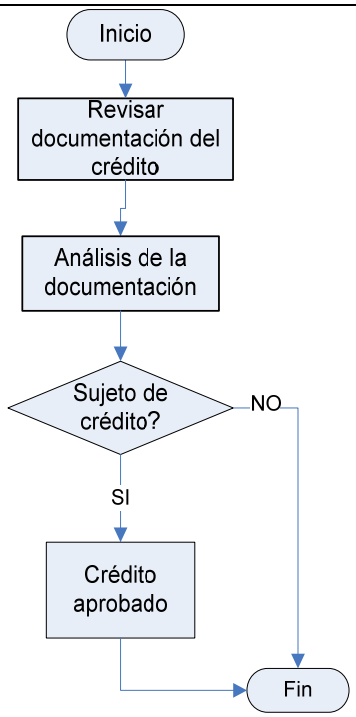
PROVEEDORES	ENTRADAS	PROCESO	SALIDA	CLIENTES
Oficial de crédito/Gerente Comité de crédito	Carpeta del socio Firmas en solicitud de petición del crédito		Crédito aprobado o negado	Socio / Oficial de crédito

Figura 2.3. Diagrama SIPOC del proceso de Aprobación del Crédito.

2.5.1.3. TERCER PROCESO (PC3): LEGALIZACIÓN DEL CRÉDITO

Objetivo del Proceso: Emisión y legalización del pagaré a la orden o contrato de préstamo como documento de respaldo de la petición de crédito aprobada por el comité de crédito.

Detalle del Proceso:

- **Elaboración de pagaré de crédito o contrato de préstamo:**
  El pagaré a la orden o el contrato de préstamo se elabora en formato word, el cual debe ser firmado por los involucrados en el crédito.
  Depende del plazo y de la forma de pago del crédito solicitado, el tipo de documento a firmarse, si el crédito está aprobado para pagarse en un solo dividendo al vencimiento de éste, se firmara un pagaré a la orden; y, si el crédito está aprobado para pagarse en cuotas ya sea de forma quincenal, mensual, bimensual o trimestral se firmará un contrato de préstamo.
  Únicamente el contrato de préstamo es legalizado ante un Notario.
- **Recepción de firmas y legalización**
  Se reciben y verifican las firmas del solicitante, garantes (de ser el caso), cónyuges y gerente de la cooperativa, en el pagaré o contrato de préstamo, el cual se legaliza ante un notario de ser caso. Tanto el pagaré a la orden como el contrato de préstamo son revisados y sumillados por asesor legal de la cooperativa.

Diagrama SIPOC del Proceso:

A continuación se emite una descripción previa al diagrama de la Figura 2.4, para una mejor comprensión del mismo.

Proveedores:

Socio: Cuenta ahorrista de la cooperativa.

Garante: Persona que respalda la operación de crédito

Garante hipotecario: Persona que respalda el crédito con su bien inmueble y con su firma.

Garante prendario: Persona que respalda el crédito con su vehículo o prenda y con su firma.

Garante con aval: Persona que respalda el crédito con su certificado de depósito de ahorro a plazo y con su firma.

Oficial de crédito: Funcionario de la cooperativa encargada de ayudar a los socios o empresas para obtener los créditos.

Gerente: Persona que está a cargo de la dirección de la cooperativa.

Notario: Funcionario cuya intervención otorga carácter público a los documentos privados, autorizándolos a tal fin con su firma y sello.

Entradas:

Pagaré o contrato de préstamo: Documento legal en donde constan las condiciones del crédito y firmas de las personas que interviene en el mismo (Anexo 5).

Cédula de Identidad: Cedula original para verificación de la firma del socio y garantes.

Firma: Da autenticidad y validez al pagaré o contrato de préstamo**.**

Nombramiento: Documento de designación del cargo de gerente el cual está legalizado ante un notario y e inscrito ante el Registro mercantil de Loja (Anexo 27).

Firma y sello de la notaría: Dan validez al contrato de préstamo.

Salidas:

Pagaré o contrato de préstamo debidamente legalizado: Documento legal en donde constan las condiciones del crédito y firmas de las personas que interviene en el mismo (Anexo 5).

Clientes:

Asesor legal: Abogado de la cooperativa que se encarga de verificar los pagarés o contratos de crédito y de recuperarlos por la vía judicial.

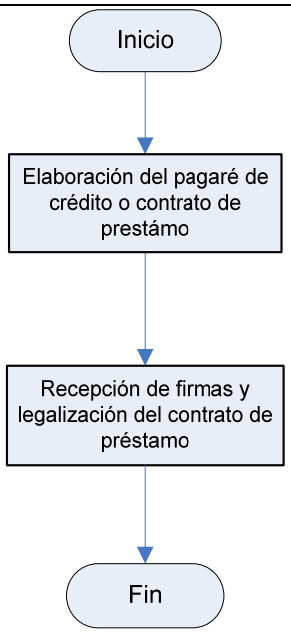
PROVEEDORES	ENTRADAS	PROCESO	SALIDA	CLIENTES
Oficial de crédito Socio Garante Gerente Notario	Pagaré o contrato de préstamo Cédula de identidad Firma Cédula de identidad Firma Cédula de identidad Firma Nombramiento Firma y sello de la notaría		Pagaré o contrato de préstamo debidamente legalizado	Asesor legal de la cooperativa

Figura 2.4. Diagrama SIPOC del proceso de Legalización del Crédito.

2.5.1.4. CUARTO PROCESO (PC4): DESEMBOLSO DEL CRÉDITO

Objetivo del Proceso: Liquidación del crédito solicitado y emisión de la tabla de amortización.

Detalle del Proceso:

- **Actualización de datos:**
  Se procede a actualizar los datos del socio en el sistema, esto se hace en la ficha de creación de cuenta que se genera al momento que el socio realiza la apertura su cuenta de ahorros.
  Se ingresa también la información del garante en la ficha respectiva, o la información de la hipoteca, prenda o aval, en la opción para estos tipos de garantía.
- **Ingreso y calificación del crédito:**
  Se registra en el sistema la información de la solicitud de crédito que presenta el socio en y luego se califica esta solicitud de crédito de igual manera en el sistema, para proceder a imprimir estos dos reportes.
- **Calculo de descuentos del crédito:**
  Se elabora una tirilla de los descuentos que se hacen al monto solicitado, el resultado de estos valores es el que será acreditado en la cuenta de ahorros del socio.
- **Desembolso del crédito:**
  Se entrega al jefe operativo toda la carpeta del socio, con los reportes y tirilla antes mencionados, para quesea revisada y en caso de que todos los ingresos de los datos

del crédito y cálculos efectuados estén correctos se proceda con el desembolso del crédito por medio de la opción respectiva en el sistema de liquidación del crédito, esta liquidación acredita el dinero del crédito en la cuenta del socio y genera una tabla de amortización que será entregada al mismo para los pagos respectivos.
Si hay algún dato que no haya sido bien ingresado o calculado se devuelve la carpeta del socio al oficial de crédito para las respectivas rectificaciones.

Diagrama SIPOC del Proceso:

A continuación se emite una descripción previa al diagrama de la Figura 2.5, para una mejor comprensión del mismo.

Proveedores:
Sistema: Software financiero utilizado en la Cooperativa de Ahorro y Crédito "Fortuna" el cual lleva el nombre de "CONEXUS".

Oficial de crédito: Funcionario de la cooperativa encargada de ayudar a los socios o empresas para obtener los créditos.

Jefe operativo: Funcionario de la cooperativa encargado de verificar los datos del crédito y desembolsar el mismo.

Entradas:
Solicitud y calificación del crédito: Opciones del sistema que permiten ingresar los datos de crédito que ha sido aprobados y permiten la calificación del mismo por medio de selección de puntajes, para que luego el crédito pueda ser liquidado**.**

Detalle de rubros de descuentos (tirilla): Cálculos realizados en una maquina sumadora, estos cálculos corresponden a los descuentos de los rubros que por ley se aplican a los créditos.

Reportes de solicitud y calificación del crédito: Documentos impresos del resultado de haber ingresado la solicitud de crédito en el sistema de haber calificado dicha solicitud también en el sistema.

Liquidación del crédito: Opción del sistema la cual permite acreditar el dinero del crédito y a la vez generar la tabla de amortización, es manejada nicamente por el jefe operativo de la cooperativa.

Salidas:
Tabla de amortización: Tabla de pagos del crédito otorgado (Anexo28).

Clientes:
Socio: Cuenta ahorrista de la cooperativa.

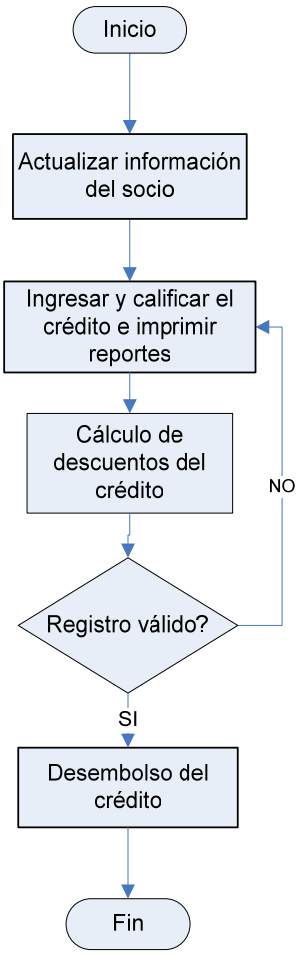
PROVEEDORES	ENTRADAS	PROCESO	SALIDA	CLIENTES
Oficial de Crédito Sistema "CONEXUS" Jefe operativo	Solicitud y calificación del crédito Detalle de rubros de descuentos(tirilla) Reportes de solicitud y calificación del crédito Liquidación del crédito		Acreditación del dinero en la cuenta del socio y generación de tabla de amortización	Socio

Figura 2.5. Diagrama SIPOC del proceso de Desembolso del Crédito.

2.5.1.5. QUINTO PROCESO (PC5): RECUPERACIÓN DEL CRÉDITO

Objetivo del Proceso: Seguimiento de pagos del crédito otorgado al socio.

Detalle del Proceso:

- **Recuperación por medio de llamada telefónica:**

  Conforme se van venciendo los créditos se realizan llamadas telefónicas del oficial, gerente y abogado, a los socios que todavía no han efectuado los pagos para que se acerquen a la cooperativa a hacerlo.

  Cuando el socio no se ha acercado a realizar el pago de la cuota del crédito luego de vencidos quince días, se procede a reportar de esto a sus garantes mediante una llamada telefónica.

  Si el socio luego de esto efectúa el pago el crédito se da por recuperado.

- **Recuperación por medio notificación escrita del oficial de crédito:**
  Si el socio no se ha acercado a efectuar el pago y ha han transcurrido treinta días, se envía un notificación escrita al deudor y a sus garantes firmada por el oficial de crédito (Anexo 6).
  Si el socio luego de esto efectúa el pago el crédito se da por recuperado.
- **Recuperación por medio notificación escrita de la gerencia:**
  Si luego de haber pasado cuarenta a sesenta y cinco días, el socio no ha realizado el pago se envía otra notificación firmada por la gerente (Anexo 6) de la cooperativa al deudor y garantes en la que se da un plazo de cuarenta y ocho horas para que realice los pagos respectivos.
  Si el socio luego de esto efectúa el pago el crédito se da por recuperado.
- **Recuperación por medio notificación escrita del asesor legal:**
  Si luego del plazo antes mencionado, el socio no se acerca a realizar el pago, se envía otra notificación firmada por el asesor legal de la cooperativa (Anexo 6) al deudor y garantes, advirtiendo que si los dividendos vencidos no son pagados en veinte y cuatro horas, el crédito será demandado judicialmente.
- **Demanda judicial:**
  Una vez que el crédito ya ha llegado a noventa días de vencido y el socio no ha realizado los pagos respectivos, se entrega el pagaré o contrato de préstamo al mediante oficio firmado por gerencia al asesor legal de la cooperativa, para que inicie el trámite de demanda judicial en el juzgado.

Diagrama SIPOC del Proceso:

A continuación se emite una descripción previa al diagrama de la Figura 2.6, para una mejor comprensión del mismo.

Proveedores:

Socio: Cuenta ahorrista de la cooperativa.

Sistema: Software financiero utilizado en la Cooperativa de Ahorro y Crédito "Fortuna" el cual lleva el nombre de "CONEXUS".

Oficial de crédito: Funcionario de la cooperativa encargada de ayudar a los socios o empresas para obtener los créditos.

Gerente: Persona que está a cargo de la dirección de la cooperativa.

Asesor legal: Abogado de la cooperativa que se encarga de verificar los pagarés o contratos de crédito y de recuperarlos por la vía judicial.

Entradas:

Tabla de amortización: Tabla de pagos del crédito otorgado (Anexo28).

Llamada: Llamada telefónica

Notificación escrita: Documento en formato word, con el cual se recuerda al socio el vencimiento de su crédito, son de tres tipos, de Oficial de crédito, de Gerencia y de Abogado (Anexo 6).

Oficio de demanda: Documento en formato word, firmado por la gerencia y entregado al asesor legal de la cooperativa solicitando se inicie el trámite de demanda del crédito vencido.

Pago del crédito: pago del dividendo o los dividendos del crédito vencido.

Salidas:

Proceso de demanda: Proceso legal llevado a cabo por el juzgado para conseguir recuperar el crédito vencido.

Clientes:

Juzgado: El tribunal de justicia o corte, es el órgano público cuya finalidad es colaborar en la recuperación del crédito.

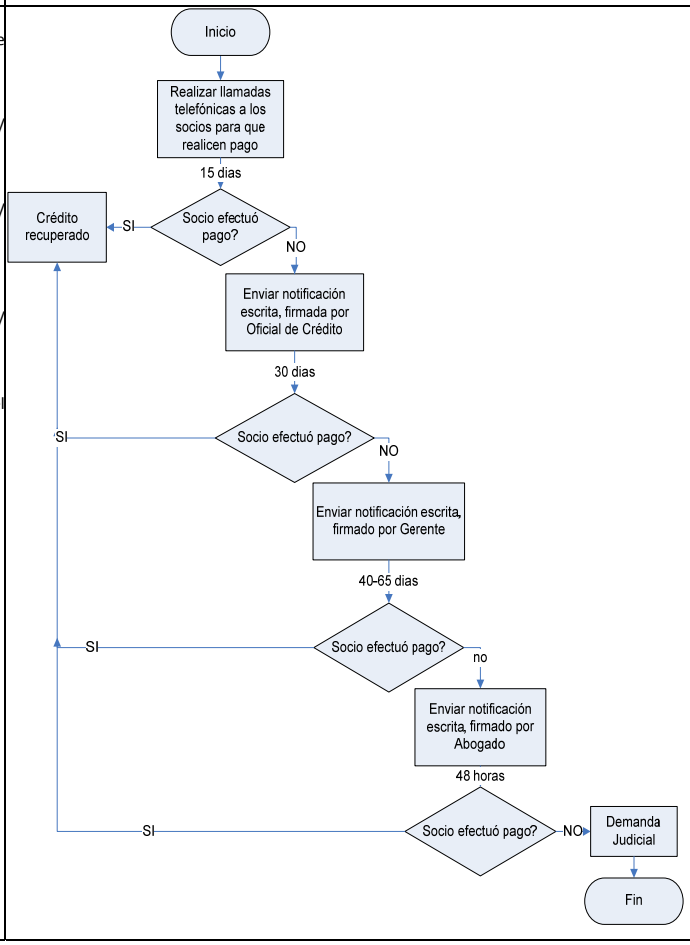
PROVEEDORES	ENTRADAS	PROCESO	SALIDA	CLIENTES
Sistema "CONEXUS" Oficial de crédito Gerente Asesor legal Socio	Tabla de amortización Llamada / Notificación escrita Llamada / Notificación escrita/Oficio de demanda Llamada / Notificación escrita Pago del crédito		Proceso de demanda	Juzgado

Figura 2.6. Diagrama SIPOC del proceso de Recuperación del Crédito.

2.6. PROCESOS COBIT QUE SE APLICARÁN EN LA AUDITORÍA

En base a los criterios de información de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento de leyes-regulaciones, y confiabilidad, que propone COBIT, se han desarrollado y aplicado encuestas para el área de gerencia (Anexo 7), el área de crédito (Anexo 8) y al área de sistemas (Anexo 9) de la cooperativa, las cuales permitieron determinar la criticidad de los procesos crediticios y de TI, y así poder establecer que procesos del marco referencial se relacionan con los procesos de crédito que se llevan a cabo en la institución.

A continuación se describen los criterios que se han tomado como guía para la selección de los procesos de COBIT y su relación con cada uno de los procesos de crédito, basándose en los dominios de control de TI de cada proceso COBIT.

- Los procesos de crédito PC1, PC2 y PC3 se relacionan con los siguientes procesos de COBIT.

  - **PO6-Cominicar las aspiraciones y la dirección de la gerencia:** La selección de este proceso radica en la importancia que tiene la definición de políticas y procedimientos de control en toda entidad, en este caso se aplica las políticas para el análisis, aprobación y legalización del crédito en la cooperativa, además se toma en cuenta que debe existir la constante comunicación con la gerencia.

  - **PO9-Evaluar y administrar los riesgos de TI:** Para este proceso se toma en cuenta la importancia de evaluar y administrar los riesgos, considerando cualquier riesgo posible en el análisis, aprobación y legalización del crédito con el fin de evitar posibles amenazas o vulnerabilidades que puedan afectar el ámbito financiero de la cooperativa.

  - **ME2-Monitorear y evaluar el control interno:** Este proceso se considera de importancia en todos los procesos de crédito ya que se debe evaluar lo correspondiente a control interno en la cooperativa, verificando el monitoreo de los controles internos, evaluando su efectividad y emitiendo reportes sobre ellos en forma regular.

  - **ME3-Garantizar el cumplimiento regulatorio:** Para estos procesos de crédito se considera de gran importancia la evaluación de las leyes y regulaciones a nivel de cooperativa para verificar si se garantiza el cumplimiento de las mismas.

- Los procesos de crédito PC4 y PC5 se relacionan con los siguientes procesos de COBIT:

  - **PO9-Evaluar y administrar los riesgos de TI:** Se considera de gran importancia la evaluación de riesgos en el desembolso y recuperación del crédito, tomando en cuenta que estos procesos tienden a ser más críticos con respecto a la situación

financiera, ya que una posible falla en el sistema ocasionaría serios problemas en la cooperativa.

- **AI4-Facilitar la operación y el uso:** Este proceso de facilidad de operación y uso, se ha considerado en los procesos de desembolso y recuperación del crédito, ya que estos se realizan en el sistema y se requiere verificar que exista la transferencia de conocimiento a usuarios involucrados, además de la constatación de si en la cooperativa se cuenta con medidas de control dirigidas a la revisión y monitoreo de acuerdos y procedimientos existentes con respecto a las políticas de la Institución en cuanto a su efectividad y suficiencia.

- **DS4-Garantizar la continuidad del servicio:** Es importante el control sobre los procesos de desembolso y recuperación del crédito con el objetivo de minimizar la probabilidad de interrupción, alteraciones no autorizadas y errores en el sistema, ya que para realizar el proceso de crédito es primordial tomar en cuenta la continuidad del servicio, verificando que en la cooperativa se cuente con los respaldos correspondientes y tener un plan de continuidad del servicio debidamente documentado y aprobado.

- **DS5-Garantizar la seguridad de los sistemas:** Se considera de importancia la Seguridad del sistema en la realización de desembolso y recuperación el crédito, con el objetivo de salvaguardar la información contra el uso, revelación o modificación no autorizada, daño o pérdida de información y determinar si existe este tipo de seguridad en la cooperativa.

- **DS11-Administrar los datos:** Se considera de importancia asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización y almacenamiento, para ello se debe verificar si la cooperativa cuenta con una combinación efectiva de controles generales y de aplicación sobre las operaciones crediticias y de TI.

- **ME2-Monitorear y evaluar el control interno:** Se considera de importancia ya que se debe realizar periódicamente la evaluación de lo adecuado del control interno en la cooperativa, incluyendo todos los procesos de crédito.

- **ME3-Garantizar el cumplimiento regulatorio:** Para todos los procesos de crédito se ha tomado en cuenta este proceso de COBIT, el cual debe satisfacer los requerimientos de la cooperativa, lo que permitirá evaluar los niveles de confianza entre la organización, los socios y proveedores externos.

La Tabla 2.3 muestra la relación existente entre cada uno de los procesos de crédito y los procesos seleccionados del marco referencial COBIT, tomando en cuenta que los tres primeros procesos de crédito son realizados manualmente y los dos últimos se los realiza por medio del sistema.

Tabla 2.3. Relación entre procesos de crédito y dominios COBIT.

PROCESOS DE CRÉDITO	DOMINIOS COBIT							
	PLANEAR Y ORGANIZAR		ADQUIRIR E IMPLEMENTAR	ENTREGAR Y DAR SOPORTE			MONITOREAR Y EVALUAR	
	PO6	PO9	AI4	DS4	DS5	DS11	ME2	ME3
PC1: Análisis del crédito	x	x					x	x
PC2: Aprobación del crédito	x	x					x	x
PC3: Legalización del crédito	x	x					x	x
PC4: Desembolso del crédito		x	x	x	x	x	x	x
PC5: Recuperación del crédito		x	x	x	x	x	x	x

CAPÍTULO 3:

APLICACIÓN DE LA AUDITORÍA INFORMÁTICA

3. *APLICACIÓN DE LA AUDITORÍA INFORMÁTICA*

Con los conocimientos obtenidos en el capítulo anterior y una vez determinados que dominios de COBIT se acogen al tema de tesis propuesto, se puede establecer una planificación orientada directamente a cada proceso de COBIT seleccionado con sus respectivas actividades y objetivos de control.

Además en esta sección se realiza la selección de las herramientas que se aplicaran en la auditoría informática, de acuerdo a sus características e importancia se ha seleccionado las herramientas IDEA para verificación de la base de datos, y NESSUS para escaneo de vulnerabilidades en los equipos correspondientes a los servidores de la cooperativa y a las terminales del área de crédito respectivamente.

3.1. DISEÑO DE INSTRUMENTOS

Se aplicará la metodología de los modelos de madurez de cada proceso de COBIT para poder determinar en qué nivel de madurez se encuentra la cooperativa "Fortuna" y en base a los resultados obtenidos poder emitir recomendaciones que ayudarán a la cooperativa a controlar de mejor manera todo lo relacionado con los procesos de crédito y de TI.

Las técnicas y herramientas seleccionadas para realizar este proceso de auditoría informática serán las siguientes:

1. **Cuestionarios**
   La aplicación de cuestionarios será realizada a gerencia, al jefe de sistemas y al oficial de crédito de la cooperativa "Fortuna".

A continuación se muestra el diseño de dichos cuestionarios:

CUESTIONARIO PARA EVALUAR EL CONTROL INTERNO DEL DEPARTAMENTO DE CRÉDITO

DE LA COOPERATIVA DE AHORRO Y CREDITO "FORTUNA"

Fecha:

Nombre del empleado: **Cargo:**

	SI	NO
Control Interno aplicado al otorgamiento de un crédito		
1. ¿La entidad cuenta con un manual o reglamento de crédito?		
2. ¿Es claro y objetivo el manual o reglamento de crédito?		
3. ¿Posee el departamento de crédito políticas establecidas?		
4. ¿Se cumplen a cabalidad las políticas de crédito en la cooperativa?		
5. ¿Existe un reglamento interno que establezca el procedimiento a seguir para otorgar los créditos?		

6. ¿Posee el departamento de crédito un manual de procedimientos que ayuda a su gestión interna?		
7. ¿Se planifica, organiza, ejecuta y controla el otorgamiento del crédito y recuperación en concordancia a la normativa interna (Reglamento de Crédito) y al organismo de control?		
8. ¿Existe un responsable de aprobar o negar los créditos a otorgar?		
9. ¿Existe una gerencia legalmente establecida para evaluar solicitudes de crédito?		
10. ¿Se realiza periódicamente la revisión de créditos por la dirección de la cooperativa?		
11. ¿Usted realiza sus actividades en el tiempo requerido?		
12. ¿Cree usted que debe existir más personal en el departamento?		
13. ¿Cuenta la cooperativa con un sistema automatizado de crédito?		
14. ¿Considera que el sistema "CONEXUS" realiza los procesos con exactitud y eficiencia?		
15. ¿Existen manuales de usuarios para el uso del sistema "CONEXUS" en lo referente a los procesos de crédito?		
16. ¿El sistema "CONEXUS" es apropiado para optimizar el uso de la información?		
17. ¿Existen controles internos en la captación de datos que no permita su manipulación indebida?		
18. ¿A la información crediticia tiene acceso cualquier empleado?		
19. ¿Se mantiene un registro actualizado de los socios en cuanto a los créditos otorgados?		
20. ¿Existe una adecuada función de supervisión de los créditos?		
21. ¿El departamento cuenta con un programa de capacitación para su personal?		
22. ¿Existen fallas de exactitud en los procesos de recolección de información?		
23. ¿Se ha establecido un procedimiento documentado para el control de los requisitos de crédito?		
24. ¿Se otorgan créditos a empresas?		
25. ¿Los procesos, políticas y procedimientos de crédito están definidos y documentados para todas las actividades?		
26. ¿Existen actas de reuniones de crédito?		
Control Interno aplicado a recuperación de crédito		
1. ¿Existe un reglamento interno que establezca el procedimiento a seguir para las cobranzas de los créditos otorgados por la cooperativa?		
2. ¿Existen formalmente políticas administrativas y legales de cobranza que permitan disminuir el índice de morosidad?		
3. ¿Existe claridad en las políticas y normas de la cooperativa en cuanto a las operaciones de cobranza?		
4. ¿Existe un manual de normas y procedimientos en el departamento de crédito?		
5. ¿Cuenta la cooperativa con un sistema automatizado de cobranzas?		
6. ¿Existe un instrumento de control para el análisis de los créditos?		
7. ¿Se lleva un control manual y sistemático de los créditos vencidos y no pagados?		

8. ¿Se mantiene un registrado actualizado de los socios en cuanto a los créditos?		
9. ¿Se controla que se envíen oportunamente las notificaciones de los avisos de vencimiento y pago de los créditos?		
10. ¿Visita a los clientes de la cooperativa que se encuentran en morosidad?		
11. ¿Revisa diariamente el comportamiento de la cartera en mora?		
12. ¿Se efectúa el seguimiento de las acciones de cobranza de la cartera, mediante mecanismos de control eficientes para su recuperación?		
13. ¿Se desarrollan e implementan estrategias para evitar riesgos crediticios, evaluando y asegurando la recuperación del crédito concedido?		
14. ¿Se informa periódicamente a Gerencia General sobre el movimiento de cartera?		
15. ¿Se organizan las actividades de promoción, colocación y recuperación del crédito?		

CUESTIONARIO PARA EVALUAR EL CONTROL INTERNO DEL ÁREA INFORMÁTICA

DE LA COOPERATIVA DE AHORRO Y CREDITO "FORTUNA"

Fecha:

Nombre del empleado: **Cargo:**

	SI	**NO**
1. ¿El sistema "CONEXUS" es apropiado para optimizar el uso de la información?		
2. ¿El sistema "CONEXUS" es adquirido a terceros?		
3. ¿El sistema "CONEXUS" cuenta tanto con el repositorio como con el diccionario de datos?		
4. ¿Existe un manual de estándares de programación en la cooperativa?		
5. ¿Existe un manual de desarrollo de aplicaciones en la cooperativa?		
6. ¿Existe un manual de funciones del departamento de sistemas?		
7. ¿Se encuentra clasificada la información del sistema "CONEXUS" de acuerdo a la criticidad?		
8. ¿Se encuentran definidos estándares dentro de TI?		
9. ¿Se encuentran definidos procedimientos para garantizar la integridad y consistencia de todos los datos almacenados en formato electrónico, tales como bases de datos, almacenes de datos y archivos?		
10. ¿Existe un monitoreo del desempeño de TI?		
11. ¿La cooperativa cuenta con requerimientos, procedimientos y políticas claras de calidad en su sistema?		
12. ¿La Cooperativa cuenta con un sistema de administración de calidad?		
13. ¿Existe un plan de contingencias de TI aprobado, difundido y probado?		
14. ¿Se han previsto riesgos de TI?		
15. ¿Se ha definido y comunicado el grado de tolerancia del riesgo en TI?		
16. ¿Se cuenta con herramientas de TI actualizadas?		
17. ¿El sistema "CONEXUS" está disponible con los requerimientos de la cooperativa?		

18. ¿Existe documentación y manuales para usuarios y para TI?		
19. ¿Considera que el sistema "CONEXUS" realiza los procesos con exactitud y eficiencia?		
20. ¿Se tiene un proceso definido para la adquisición y mantenimiento de software?		
21. ¿Existe un monitoreo del servicio prestado por proveedores de TI?		
22. ¿Han existido problemas en la instalación del software financiero luego de haberse aprobado su utilización?		
23. ¿Se cuenta con un listado de empresas idóneas proveedoras de servicios de TI?		
24. ¿Los proveedores de aplicaciones brindan la capacitación respectiva?		
25. ¿Los equipos de computación soportan los programas a instalarse?		
26. ¿El usuario final es considerado en las pruebas del software?		
27. ¿El usuario certifica las pruebas antes de pasar a producción?		
28. ¿Se cuenta con una definición documentada de acuerdos de servicios de TI de niveles de servicio?		
29. ¿Se han definido y puestos en conocimiento los niveles de servicio de TI?		
30. ¿Se han establecido convenios de servicios entre el área de TI y los usuarios?		
31. ¿Existe un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI?		
32. ¿Se ha evaluado la pérdida económica cuando puede existir una falta en la continuidad del negocio?		
33. ¿Existen equipos de respaldo que permite reanudar las actividades?		
34. ¿A la información tiene acceso cualquier empleado?		
35. ¿Se han definido políticas en cuanto a la seguridad informática?		
36. ¿Se encuentra en los contratos del personal de TI una cláusula que determine la confidencialidad?		
37. ¿Se tienen identificados los archivos con información confidencial y se cuenta con claves de acceso?		
38. ¿Cuenta con infraestructura para el control de acceso a Internet?		
39. ¿Existe un adecuado control de virus informáticos?		
40. ¿Existe un proceso de administración de incidentes?		
41. ¿Se tiene registros de problemas y la revisión del estatus de las acciones correctivas?		
42. ¿Se efectúan respaldos de la información?		
43. ¿Se cuenta con estándares de representación de datos?		
44. ¿Existen procedimientos de respaldos y recuperación de información?		
45. ¿Se cuenta con contratos de mantenimiento de equipos de computación?		
46. ¿Existen evaluaciones a los clientes internos del área de TI?		
47. ¿Se efectúa un control interno al área de TI?		

CUESTIONARIO PARA EVALUAR EL CONTROL INTERNO DE GERENCIA

DE LA COOPERATIVA DE AHORRO Y CREDITO "FORTUNA"

Fecha:

Nombre del empleado: **Cargo:**

	SI	NO
1. ¿Los usuarios conocen las políticas institucionales?		
2. ¿Se cuenta con procedimientos que permita evaluar y priorizar requerimientos para establecer soluciones de TI (Tecnología de información)?		
3. ¿Las soluciones de TI están definidas de acuerdo a la actividad que realiza la cooperativa?		
4. ¿Se han encaminado los recursos de la cooperativa en tecnología acorde a sus necesidades?		
5. ¿Existen actas de reuniones del área de TI para evaluar las actividades que presta la misma?		
6. ¿Se generan reportes gerenciales que permitan evaluar al área de TI?		
7. ¿Se realiza periódicamente la revisión de la documentación por la dirección de la cooperativa?		
8. ¿Existe en la cooperativa un Comité de Auditoría?		
9. ¿Los empleados de la cooperativa conocen claramente sus funciones y responsabilidades en el departamento que laboran?		
10. ¿Se conocen las leyes y regulaciones aplicadas a nivel de crédito?		
11. ¿Cuenta la cooperativa con un código de ética?		
12. ¿La cooperativa tiene definido un plan de capacitación a sus empleados?		
13. ¿Existe en la cooperativa un departamento de auditoría interna?		

2. **Listas de chequeo**

   Las listas de chequeo a usarse serán del tipo binario y formaran parte de una matriz de evaluación, la cual, en base a las repuestas seleccionadas permitirá obtener el nivel de madurez actual en el que se encuentra la cooperativa en cuanto a lo que establecen los procesos de cada dominio de COBIT.

   La matriz de evaluación (Anexo 22), por la extensión de dicha matriz ha sido necesario incluirla en un anexo) permitirá obtener información de evidencias, localización de estas evidencias y las observaciones o conclusiones de esta evaluación, lo que ayudara a una correcta descripción de puntos débiles y punto fuertes de los procesos en la cooperativa.

3. **Paquete de análisis de vulnerabilidades de la red (NESSUS)**

   La interfaz de usuario NESSUS permitirá analizar los servidores de la cooperativa, así como las terminales de crédito, esta herramienta

generará reportes con los datos de las vulnerabilidades y las políticas de exploración, y emitirá una lista de los objetivos y resultados de los análisis los cuales se almacenarán en un único archivo, el cual se podrá exportar fácilmente. Al ser NESSUS independientemente de la plataforma base se podrá usar sin problemas en los servidores como en las terminales que serán analizadas en esta auditoría.

4. **Paquetes de auditoría (IDEA).**
   Es un software especial para la auditoría informática, el cual admitirá especificaciones de auditoría para organizar, combinar, calcular y analizar datos de la base de datos de la cooperativa.
5. **Observación**
   Esta técnica permitirá cerciorarse de cómo se ejecutan las operaciones, como están los activos y documentos, con el objeto de establecer su existencia y autenticidad. La observación hará más confiable la obtención de la información y evidencias.

También se emplearán los siguientes recursos:

- **Recursos materiales**
  - Recursos materiales software: Programas propios de la auditoría, muy potentes y flexibles.
  - Recursos materiales hardware: Activos que el auditor necesitará y que serán proporcionados por la cooperativa, para lo cual habrá de convenir tiempo de máquina, espacio de disco, impresoras, etc.
- **Recursos humanos**
  El auditor y personal entrevistado.

3.2. ESTUDIO Y SELECCIÓN DE HERRAMIENTAS DE VALIDACIÓN

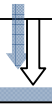
De las herramientas de auditoría mencionadas en el capítulo 1, se ha usado IDEA para realizar la verificación de los datos que se encuentran en la base de datos de la cooperativa "Fortuna", y también se ha empleado la herramienta NESSUS para evaluar la seguridad en la red y realizar la búsqueda de vulnerabilidades en el servidor y en las terminales de crédito.

3.3. PROCESO DE LA AUDITORÍA

A continuación se detalla el proceso de auditoría realizado:

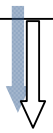
PLANIFICACIÓN DE LA AUDITORÍA INFORMÁTICA

- Definición de los objetivos y alcance de la auditoría
- Designación del equipo auditor
- Determinación de los involucrados en la auditoría
- Obtención de información detallada de los procesos a auditar, los cuales se seleccionaron por medio de una matriz de probabilidad de ocurrencia
- Selección de los procesos COBIT a aplicarse en la auditoría por medio de la aplicación de encuestas al departamento de crédito, gerencia y sistemas (Anexo 7, Anexo 8, Anexo 9)
- Estudio y selección de instrumentos, herramientas y metodologías a usar en la auditoría



EJECUCIÓN DE LA AUDITORÍA INFORMÁTICA

- Las herramientas seleccionadas para la ejecución de la auditoría son IDEA y NESSUS
- Mediante la ejecución de DEA se podrá auditar la base de datos mediante las funciones que ésta posee
- Mediante la aplicación de NESSUS se podrá determinar las vulnerabilidades de los servidores y las terminales de crédito mediante la emisión de un reporte
- Se aplicará la metodología de niveles de madurez de cada uno de los ocho procesos COBIT seleccionados (ver Tabla 2.3), para ello se usará una matriz de evaluación (Anexo 22), esta matriz está realizada en formato Excel y compuesta por una lista de chequeo con los criterios que establece COBIT por cada proceso y su nivel de madurez , éstos criterio son encuestados a las funcionarias de crédito, sistemas y gerencia de la cooperativa, y sus respuestas más la observación, recopilación y verificación de evidencias por cada actividad efectuada, permitirán determinar el nivel de madurez actual de los procesos de crédito de la cooperativa, los cuales se presentaran el tablas y mediante una gráfica de niveles versus procesos.



FINALIZACIÓN DE LA AUDITORÍA INFORMÁTICA

- Se analizarán los hallazgos encontrados, determinando los puntos fuertes y puntos débiles de la cooperativa, en los procesos evaluados.
- Se emitirá un plan de acción a seguir para mejorar o cambiar las falencias de la institución
- Se emitirá el informe final de auditoria

Figura 3.1. Proceso de la Auditoría

3.3.1. APLICACIÓN DE NESSUS

La herramienta NESSUS[6], permite la configuración de opciones como políticas que se pueden especificar de acuerdo a los requerimientos del escaneo de vulnerabilidades. El objetivo de realizar la auditoría en seguridad, es encontrar las falencias existentes en lo referente a controles de accesos no autorizados a la red. [64]

COMPONENTES DE LA HERRAMIENTA:

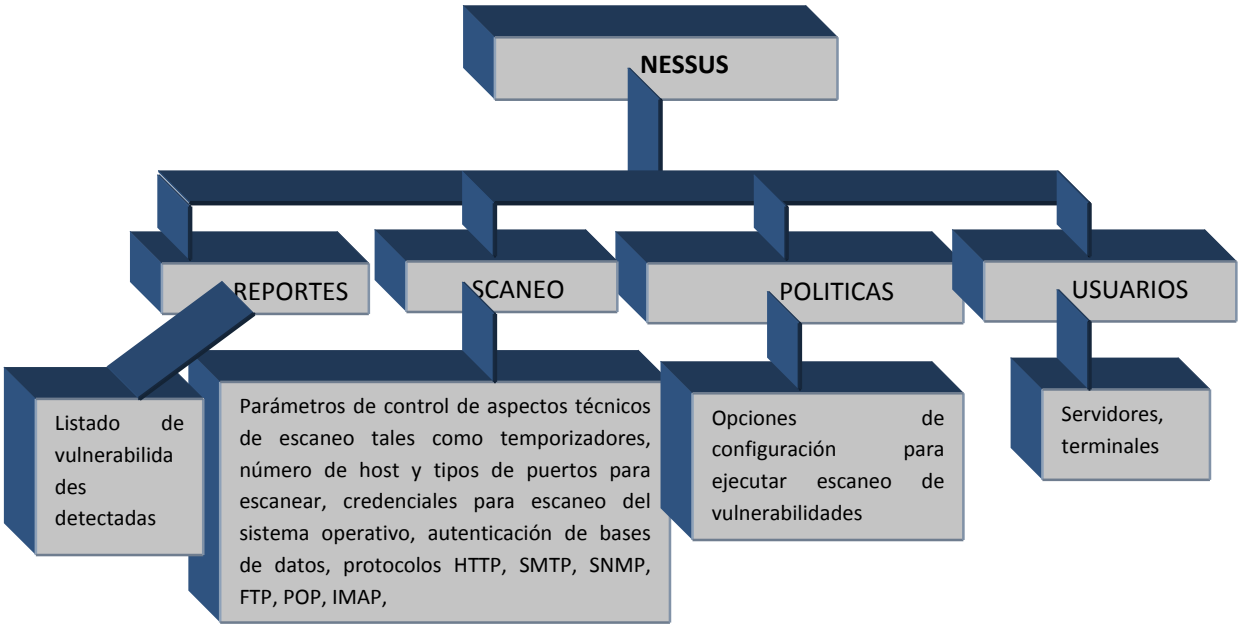


Figura 3.2.Componentes de NESSUS

[6] Fuente: Guía de Instalación, Disponible en: http://static.tenable.com/documentation/nessus_4.4_installation_guide.pdf.

INSTALACIÓN Y CONFIGURACION:

Descargar la última versión de NESSUS en: http://www.nessus.org/download/

Realizar la instalación de la herramienta en base a la guía de instalación.

Una vez realizada la instalación de la herramienta NESSUS, se realiza la configuración.

Para iniciar, parar y configurar el Servidor NESSUS, se usa el NESSUS Server Manager, permitiendo realizar lo siguiente:

- Registrar el Servidor NESSUS en nessus.org para recibir plugins actualizados.
- Ejecutar un plugin actualizado.
- Administrar usuarios de NESSUS.
- Iniciar o parar el Servidor NESSUS.

Para realizar las acciones mencionadas anteriormente ir a **Inicio/Todos los programas/Tenable network security/Nessus64/Nessus Server Manager/** y aparecerá la ventana principal, como se muestra en la Figura 3.3**.** Además se debe obtener el código de activación que será enviado al correo electrónico registrado[7], luego ingresar el código y hacer clic en **Register**, para que se active la acción **Start Nessus Server**.

Se debe cambiar el puerto de Nessus por defecto, para eso es necesario editar el archivo **nessusd.conf** que está localizado en **C:\Program Files\Tenable\Nessus\conf**,y se deben configurar los parámetros, como se muestra en la Tabla 3.1.

Se realizará el análisis de vulnerabilidades a los servidores y a los equipos pertenecientes al área de crédito, cuyos IP también de detallan en laTabla 3.1.

Tabla 3.1. Parámetros de configuracion de NESSUS.

PARÁMETRO A CONFIGURAR	VALOR DEL PARÁMETRO
Puerto para el cliente NESSUS	1241
Puerto para el servidor web NESSUS	8834
IP del servidor de base de datos	192.100.X.X
IP del servidor DNS	192.168.X.X
IP del equipo de crédito1	192.168.X.X
IP del equipo de crédito2	192.168.X.X
Base de datos	Informix
Port Scan	Tcp

[7] Fuente: Pagina de registro para obtener código de activación: Disponible en: http://www.nessus.org/plugins/?view=register-info.

Después de cambiar estos valores, parar el servicio de NESSUS vía el Server Manager y reiniciar el programa.

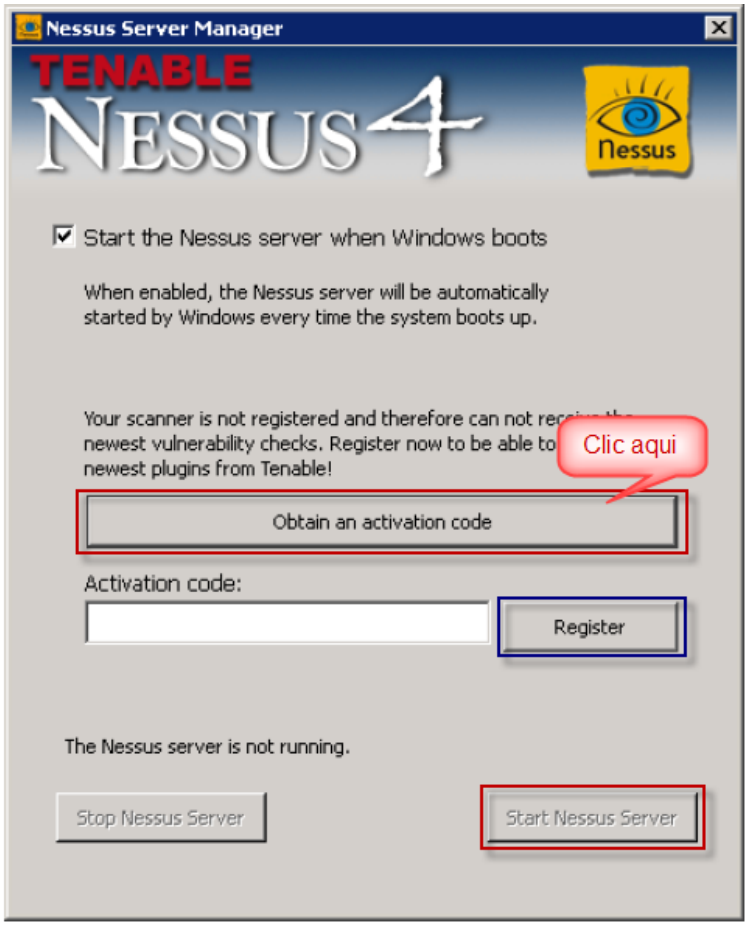


Figura 3.3. Pantalla principal de NESSUS.

Una vez registrado el NESSUS Server Manager y obtenidos los plugins aparecerá la siguiente ventana, como se muestra en la Figura 3.4.

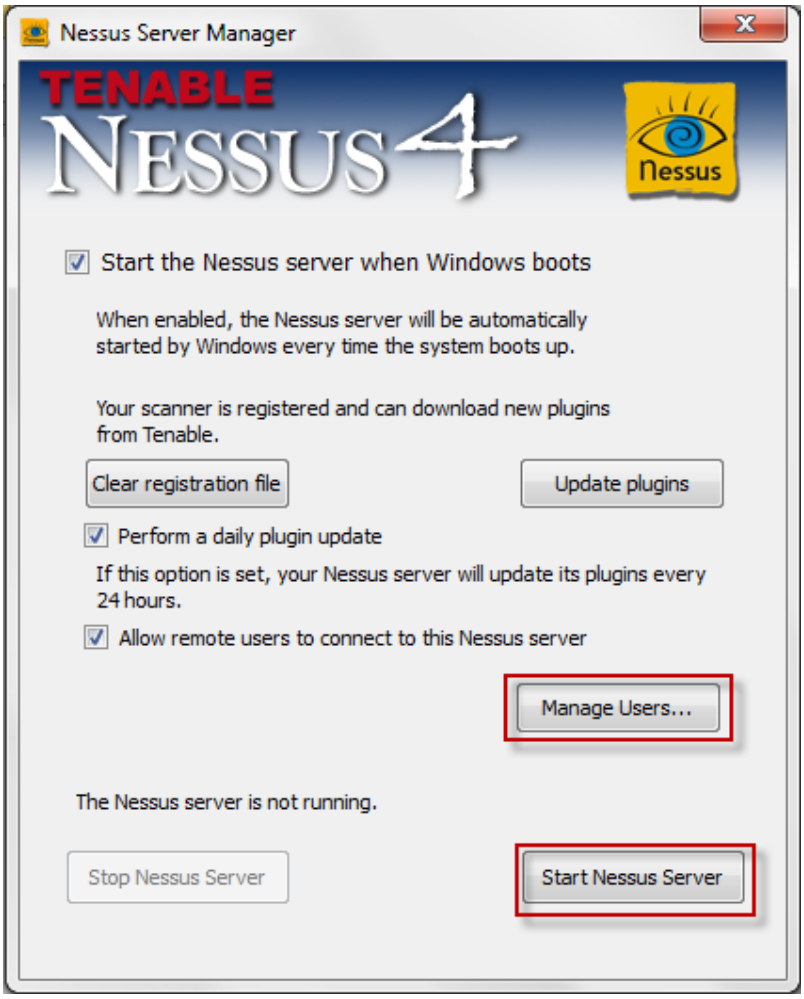


Figura 3.4. Ventana principal con plugins obtenidos.

Para crear y administrar cuentas de usuarios en NESSUS se ubica en Manage Users… , aparecerá una ventana que permite añadir o editar una nueva cuenta de usuario, para esto hacer clic en el signo [+], donde aparece una nueva ventana para ingresar el nombre de usuario y contraseña, se debe seleccionar la opción **Administrator** y luego clic en **Save** para guardar el nuevo usuario creado, como se muestra en la Figura 3.5.

Además seleccionando un nombre de la lista y haciendo clic en **Edit** se puede cambiar la contraseña del usuario y haciendo clic en [-] se puede eliminar el usuario seleccionado.

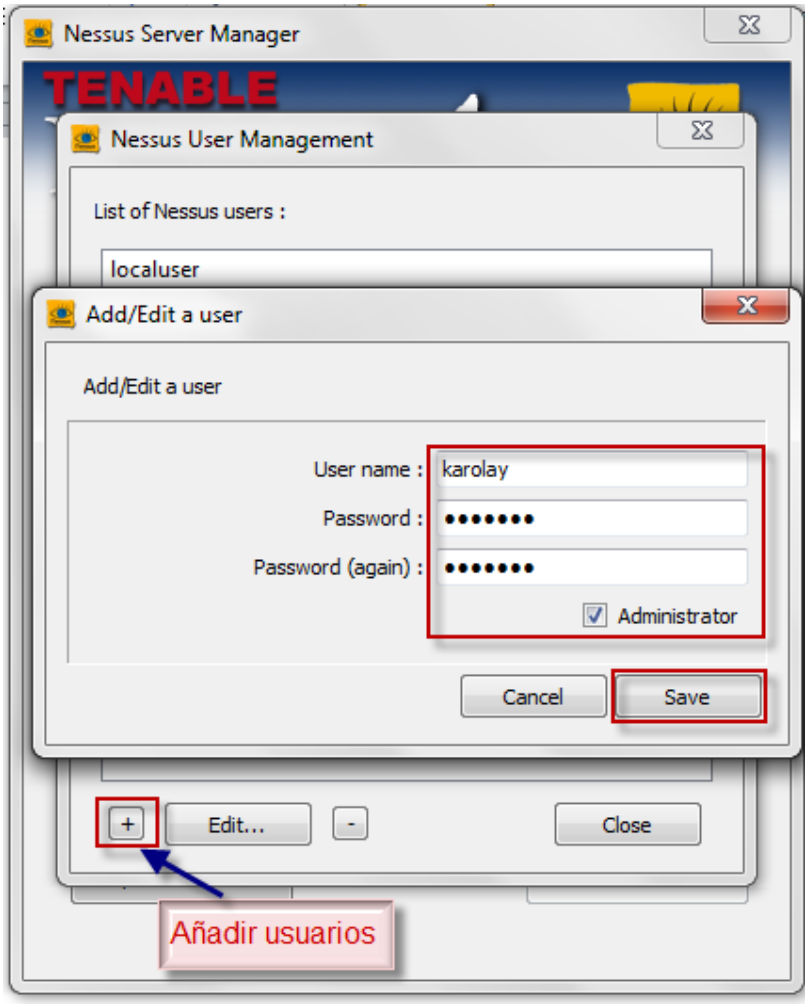


Figura 3.5. Proceso de creación de un nuevo usuario.

Si el demonio de NESSUS no está corriendo o la interfaz de usuario no está disponible, el buscador web daría un mensaje de error indicando que no se puede conectar.

Si el puerto 8834 está en estado LISTENING, ya se tendrá acceso al servidor web, para luego de acceder al servidor web, donde se solicita usuario y contraseña previamente creada en el Server Manager.

Después de la autenticación satisfactoria, se muestra el menú de opciones de la Figura 3.6.

Figura 3.6. Ingreso a NESSUS Client.

PLAN DE PRUEBAS A USAR:

¿Qué se va a evaluar con NESSUS?

- Seguridad en la red (detección de vulnerabilidades).
- Seguridad en el servidor (detección de vulnerabilidades).
- Seguridad en el sistema operativo. (detección de vulnerabilidades del S.O)
- Seguridad en la base de datos.

PERSONALIZACION Y ENTORNO DE PRUEBAS:

A continuación se detalla la aplicación de NESSUS:

El siguiente paso es crear una política, para ello se ubica en la pestaña **Policies** y luego en **Add**, aparecerá una nueva ventana que solicitan ingresar información necesaria para crear la política y luego clic en **Next**, el proceso se muestra en la Figura 3.7.

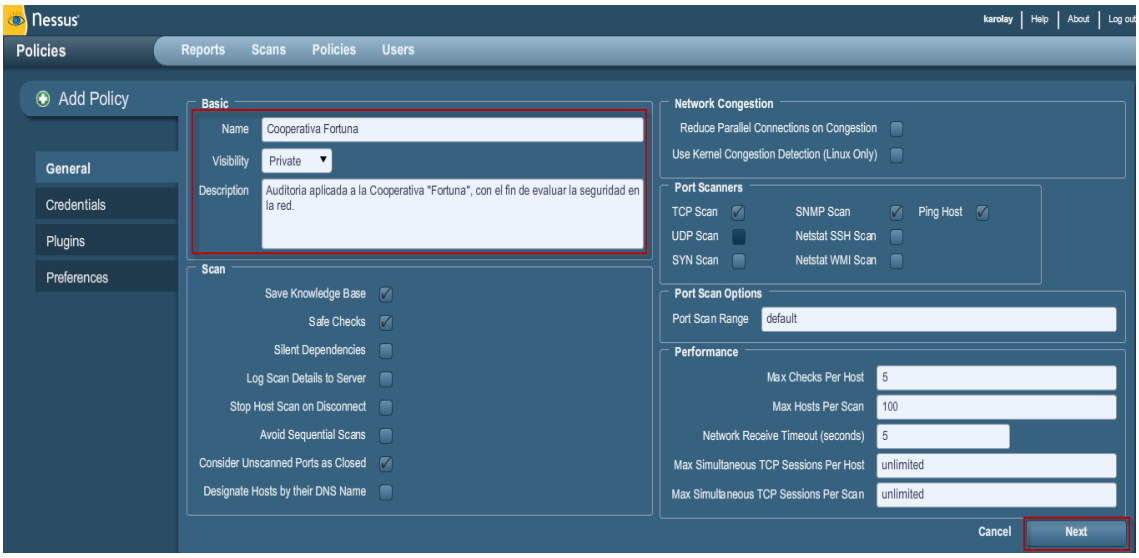


Figura 3.7. Política creada para la cooperativa "Fortuna".

A continuación se selecciona información de las pestañas **Credentials** como se muestra en la Figura 3.8.

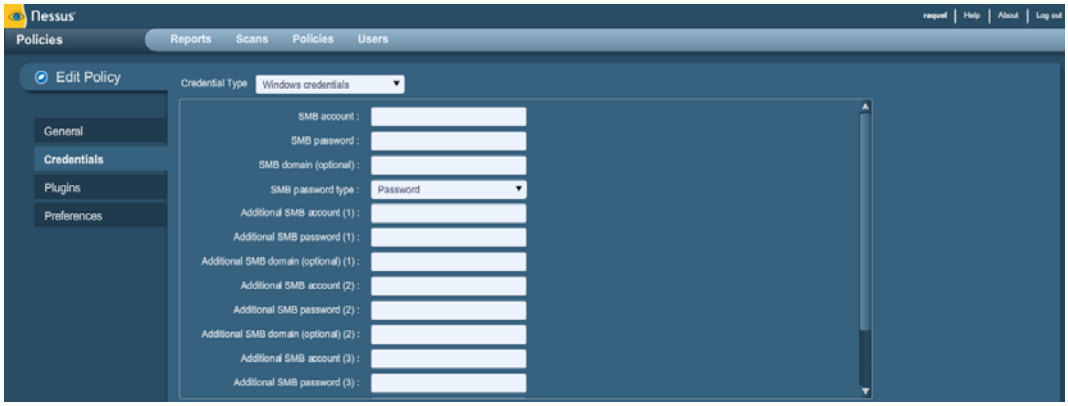


Figura 3.8.Información de Credentials.

La Figura 3.9, muestra información de los **Plugins,** se puede filtrar y seleccionar los plugins necesarios.

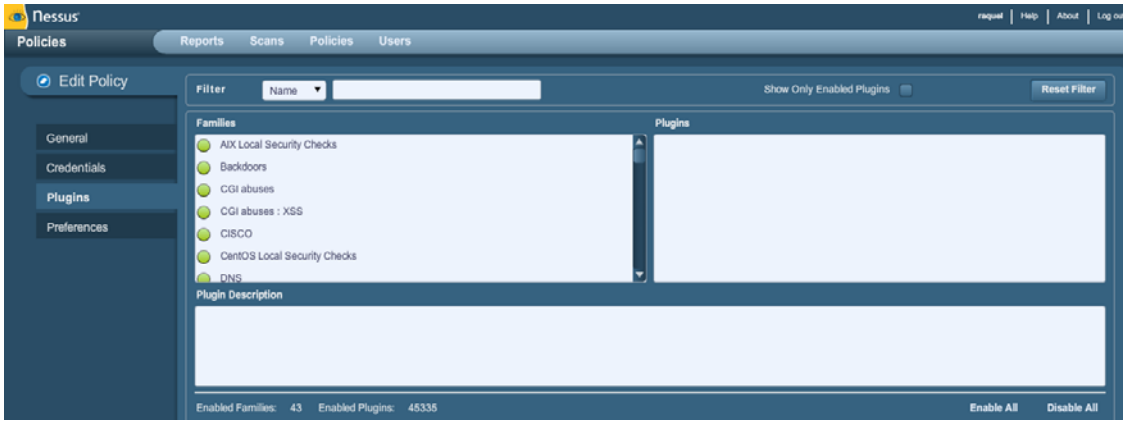


Figura 3.9. Información de Plugins.

Luego en **Preferences** se selecciona el tipo de base de datos que se utiliza, en este caso es Informix y finalmente en **Submit** para crear la política. El proceso se realiza en la Figura 3.10.

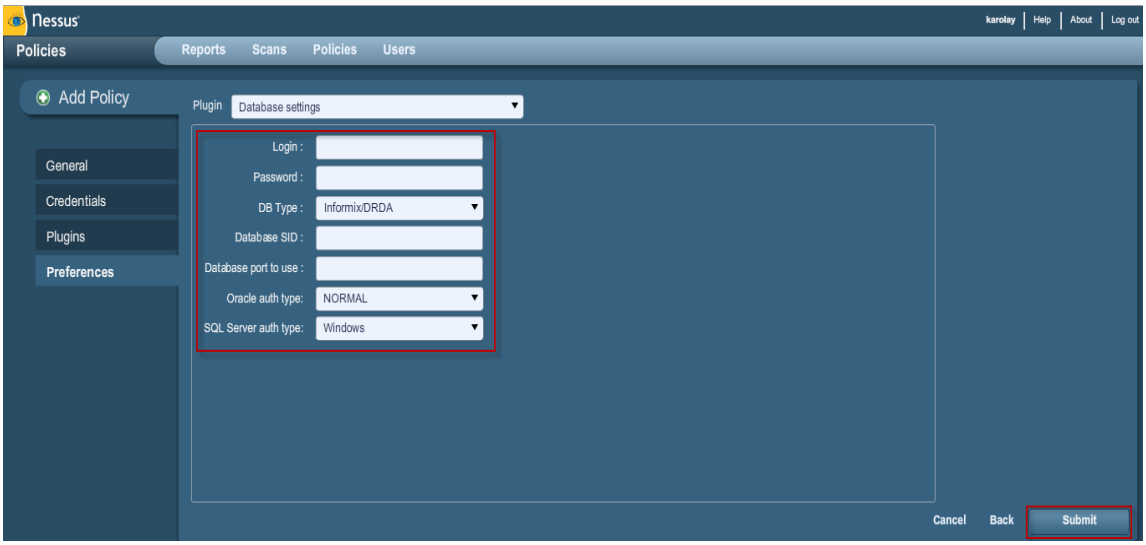


Figura 3.10. Selección de tipo de base de datos en Preferences.

Una vez creada la política, ubicarse en la pestaña **Scans** y luego en **Add** para añadir un scan, donde se asigna un nombre, se selecciona la política creada en el paso anterior y se añade las direcciones IP de los equipas que se va escanear. Selecciona **Lauch Scan** para iniciar, como se refleja en la Figura 3.11.

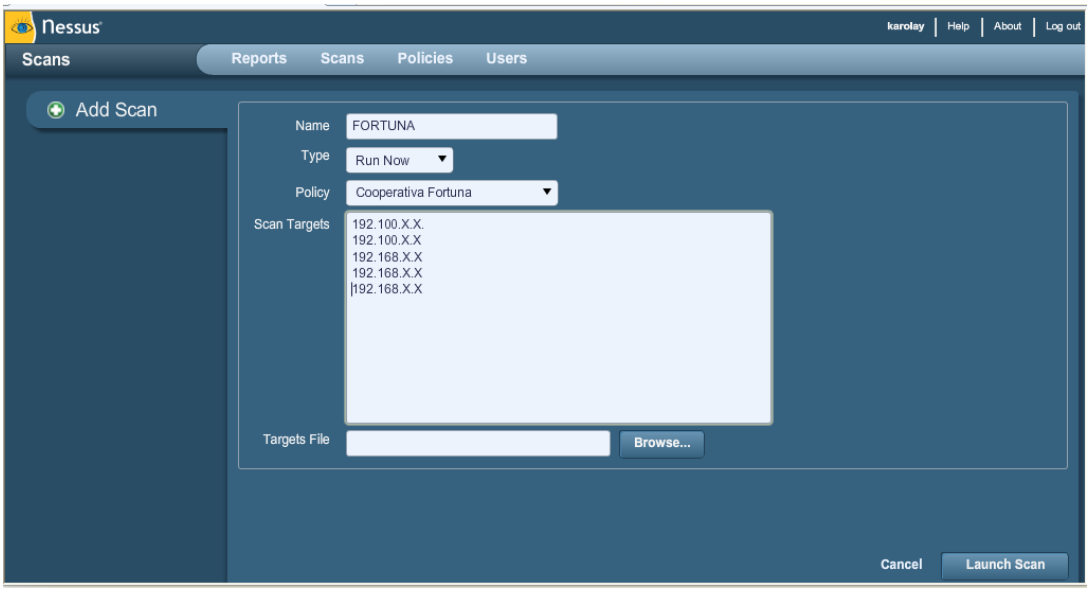


Figura 3.11. Creación de nuevo scan.

Finalmente en la pestaña **Reports,** Figura 3.12, muestra los **Scans** que se realizó en el paso anterior (por motivos de seguridad no se presentan las direcciones IP completas).

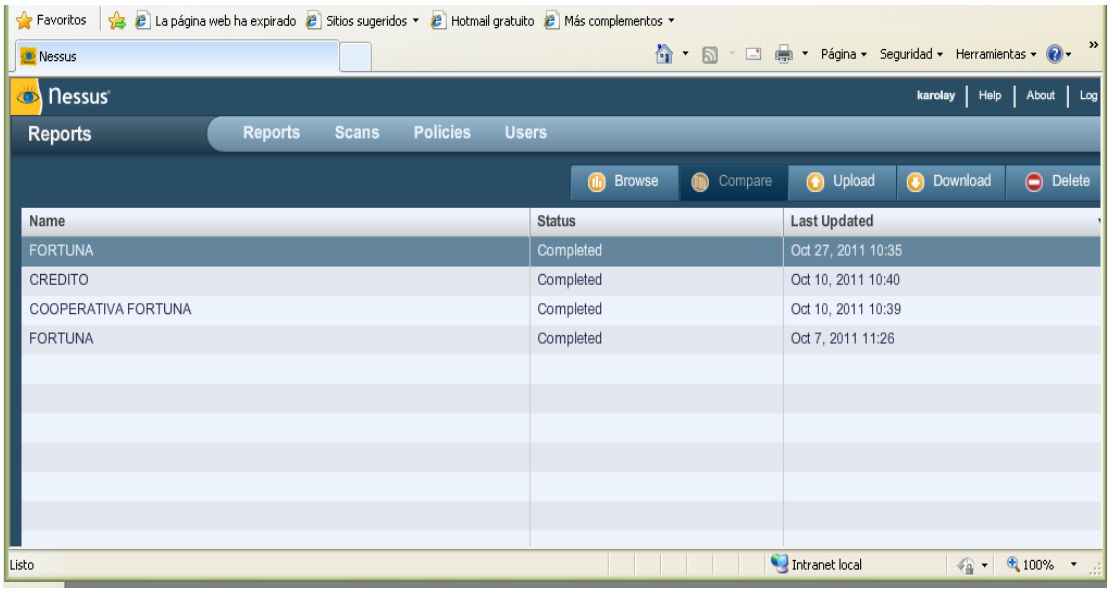


Figura 3.12. Información de scan realizado.

RESULTADOS:

Seguidamente se puede visualizar en la Figura 3.13, las vulnerabilidades encontradas con alto, medio y bajo nivel de riesgo.

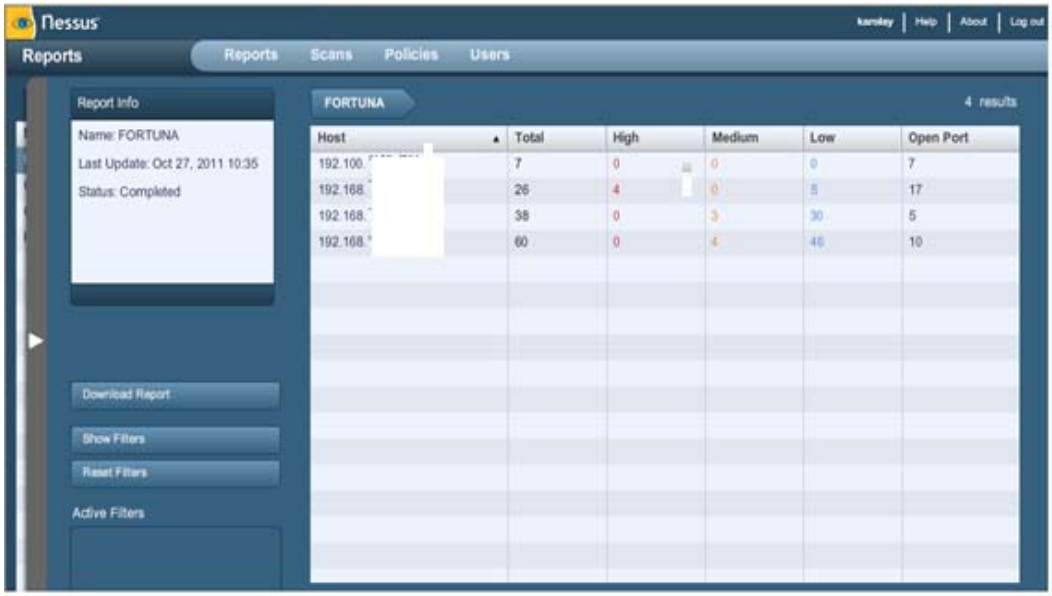


Figura 3.13. Información de vulnerabilidades encontradas.

Luego para obtener el reporte completo de las vulnerabilidades encontradas se hace clic en Download Report como se observa en la Figura 3.14, y finalmente se obtiene un reporte de vulnerabilidades que se lo puede leer en formato Word y que se resume en la Tabla 3.2 y

Tabla 3.3.

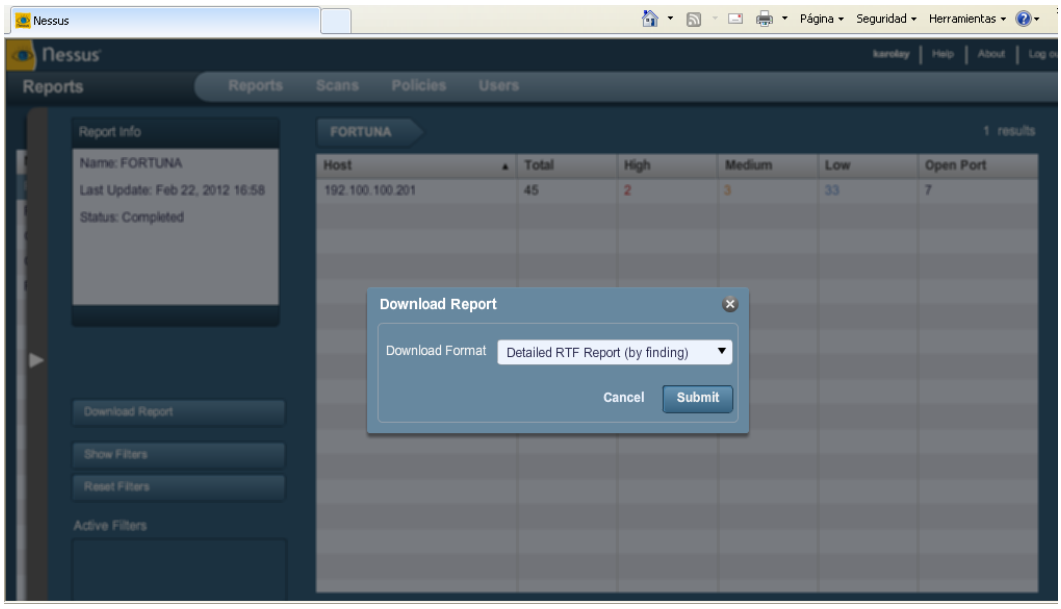


Figura 3.14. Obtención del reporte de vulnerabilidades

Tabla 3.2. Detección de vulnerabilidades en el servidor de Base de Datos y servidor DNS.

PLUGIN ID#	#	PLUGIN NAME	SEVERITY
34460	2	Obsolete Web Server Detection	High Severity problem(s) found
47709	1	Microsoft Windows 2000 Unsupported Installation Detection	High Severity problem(s) found
42411	1	Microsoft Windows SMB Shares Unprivileged Access	High Severity problem(s) found
36036	1	Conficker Worm Detection (uncredentialed check)	High Severity problem(s) found
35362	1	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)	High Severity problem(s) found
22194	1	MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)	High Severity problem(s) found
22034	1	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check)	High Severity problem(s) found
21193	1	MS05-047: Plug and Play Remote Code Execution and Local Privilege Elevation (905749) (uncredentialed check)	High Severity problem(s) found
19408	1	MS05-039: Vulnerability in Plug and Play Service Could Allow Remote Code Execution (899588) (uncredentialed check)	High Severity problem(s) found

19407	1	MS05-043: Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) (uncredentialed check)	High Severity problem(s) found
56211	2	SMB Use Host SID to Enumerate Local Users Without Credentials	Medium Severity problem(s) found
56210	2	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration Without Credentials	Medium Severity problem(s) found
45517	1	MS10-024: Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service (981832) (uncredentialed check)	Medium Severity problem(s) found
26920	1	Microsoft Windows SMB NULL Session Authentication	Medium Severity problem(s) found
18602	1	Microsoft Windows SMB svcctl MSRPC Interface SCM Service Enumeration	Medium Severity problem(s) found
18585	1	Microsoft Windows SMB Service Enumeration via \srvsvc	Medium Severity problem(s) found
12218	1	mDNS Detection	Medium Severity problem(s) found
11213	1	HTTP TRACE / TRACK Methods Allowed	Medium Severity problem(s) found
10079	1	Anonymous FTP Enabled	Medium Severity problem(s) found
22964	8	Service Detection	Low Severity problem(s) found
22319	4	MSRPC Service Detection	Low Severity problem(s) found
11111	4	RPC Services Enumeration	Low Severity problem(s) found
11011	4	Microsoft Windows SMB Service Detection	Low Severity problem(s) found
24260	3	HyperText Transfer Protocol (HTTP) Information	Low Severity problem(s) found
54615	2	Device Type	Low Severity problem(s) found
45590	2	Common Platform Enumeration (CPE)	Low Severity problem(s) found
25220	2	TCP/IP Timestamps Supported	Low Severity problem(s) found
19506	2	Nessus Scan Information	Low Severity problem(s) found

Tabla 3.3. Detección de vulnerabilidades en los equipos del área de crédito.

PLUGIN ID#	#	PLUGIN NAME	SEVERITY
51192	2	SSL Certificate signed with an unknown Certificate Authority	Medium Severity problem(s) found
26920	2	Microsoft Windows SMB NULL Session Authentication	Medium Severity problem(s) found
26919	2	Microsoft Windows SMB Guest Account Local User Access	Medium Severity problem(s) found
12218	1	mDNS Detection	Medium Severity problem(s) found
22964	9	Service Detection	Low Severity problem(s) found
11011	4	Microsoft Windows SMB Service Detection	Low Severity problem(s) found
54615	2	Device Type	Low Severity problem(s) found
53491	2	SSL / TLS Renegotiation DoS	Low Severity problem(s) found
45590	2	Common Platform Enumeration (CPE)	Low Severity problem(s) found
35716	2	Ethernet Card Manufacturer Detection	Low Severity problem(s) found

Para mayor detalle en el Anexo 23, se halla el reporte completo de las vulnerabilidades encontradas así como una posible solución para cada una de ellas, en base al plugins asociado de acuerdo a los resultados obtenidos de la ejecución de NESSUS en el servidor de base de datos, el servidor DNS, y en las terminales de crédito.

A continuación se resumen las vulnerabilidades de mayor índice de riesgo, específicamente las de nivel alto y nivel medio.

- El sistema operativo del servidor DNS es obsoleto, ya que está corriendo en una versión de Microsoft Windows 2000, la misma que ya no tiene soporte para las vulnerabilidades existentes.
- Se puede acceder a un recurso compartido de red usando una sesión nula, permitiendo a un atacante leer o escribir los datos confidenciales.
- Los servidores parecen estar infectados por algunos tipos de gusanos que podrían propagarse a otros host y permitir a un atacante ejecutar código malicioso debido a la falla de algunos servicios.
- Emulando llamadas a ciertas funciones es posible obtener el SID del servidor sin credenciales, este puede ser usado para conseguir la lista de usuarios locales. Además se podría obtener información del equipo como: tipo de S.O y versión exacta, nombre del host y lista de servicios propios del sistema que están corriendo.

- El servidor permite logins con texto claro permitiendo a los atacantes manejar usuarios y contraseñas por sniffing de tráfico al servidor, los host tienen contraseñas configuradas para que nunca expiren y los controles de seguridad local están desactivados.
- Entre las recomendaciones principales otorgadas por NESSUS se mencionan que: se desactiven los servicios propios del sistema operativo si no son necesarios, se actualice el sistema operativo a una nueva versión, se actualice el antivirus y realizar un scan completo al sistema operativo de los equipos.

De acuerdo a los resultados obtenidos se puede concluir que la mayoría de las vulnerabilidades encontradas han sido en los equipos que tienen instalado el sistema operativo Windows, ya que el servidor de base de datos está en Linux y no se han encontrado mayores riesgos posibles.

3.3.2. APLICACIÓN DE IDEA

IDEA[8] es una herramienta que ayuda a auditores y profesionales de sistemas y finanzas.

IDEA permite leer diferentes tipos de archivos entre ellos Excel, lo que facilitará el análisis de la base de datos de la cooperativa, debido a que el sistema que maneja la Institución permite exportar reportes de la base de datos con este formato.

Características

IDEA permite:

- Importar datos desde un amplio rango de tipos de archivo.
- Crear vistas personales de los datos y los reportes.
- Llevar a cabo análisis específicos de los datos como el cálculo de estadísticas diversas, detección de omisiones, detección de duplicados y sumarizaciones.
- Efectuar diversidad de cálculos.
- Obtener muestras usando diversas técnicas de muestreo.
- Unir y comparar diferentes archivos de datos.
- Cuenta con funciones para aritmética, textos, fechas y horas, e incluso funciones financieras, que permiten ejecutar operaciones con fechas, cálculos financieros y estadísticos.
- Diseñar reportes.

[8] Fuente: http://www.caseware-idea.com/

COMPONENTES DE LA HERRAMIENTA:

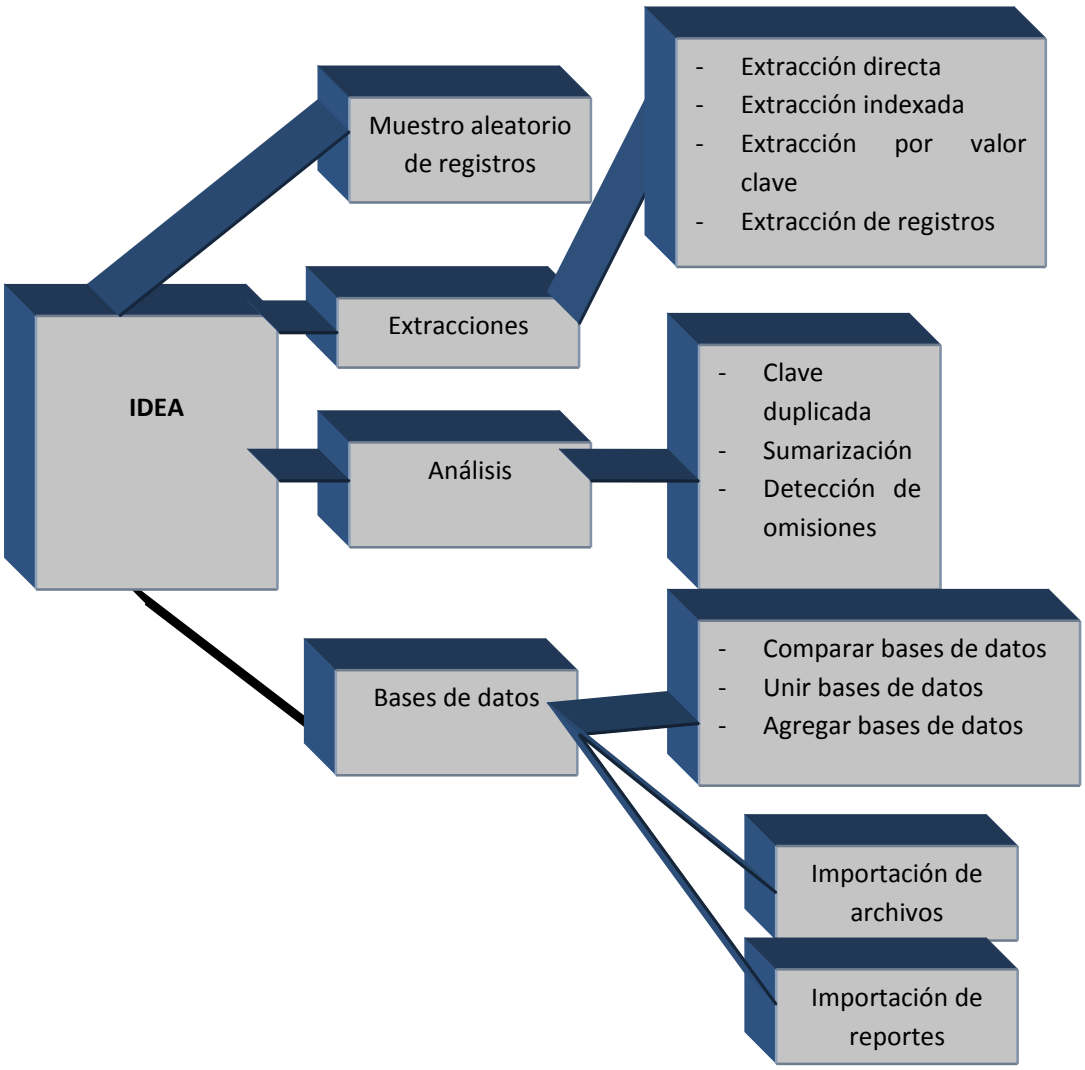


Figura 3.15. Componentes de IDEA.

INSTALACIÓN Y CONFIGURACION:

Descargar la última versión de IDEA en: http://www.caseware-idea.com/

Realizar la instalación de la herramienta en base a la guía de instalación[9],

PLAN DE PRUEBAS A USAR:

¿Qué se va a evaluar con IDEA?

[9] Fuente: Guía de Instalación, Disponible en: http://es.scribd.com/doc/55192739/Installation-Guide

- **Consistencia de información**
  - Límite de créditos.
  - Evaluar si los cálculos de intereses de mora son correctos
  - Totalizar las cuotas y días de mora por cliente para obtener los socios demandados
- **Redundancia**
  - Datos clave duplicados (créditos con el mismo número de operación).
- **Validez**
  - Verificar que no haya operaciones en fechas inusuales
- **Integridad**
  - Verificar que en las secuencias de los números de créditos no existan omisiones

PERSONALIZACION Y ENTORNO DE PRUEBAS:

Para la aplicación de esta herramienta se han tomado datos de reportes obtenidos de la base de datos de la cooperativa.

Los reportes contienen datos de créditos otorgados desde Enero del 2004 hasta Septiembre del 2011, ya que IDEA permite analizar volúmenes grandes de registros se tomado como muestra el universo, es decir todos los registros existentes.

Una vez realizada la instalación de la herramienta IDEA de acuerdo a la guía de instalación, se puede visualizar información de las bases de datos, como se muestra en la Figura 3.16.

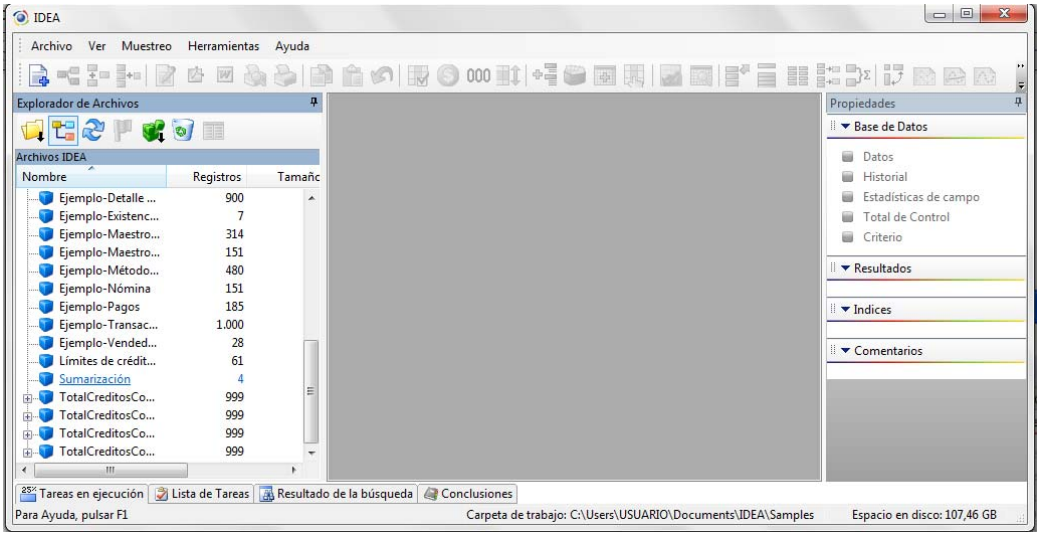


Figura 3.16. Ventana principal de IDEA.

El siguiente paso es importar archivos de Excel para ser analizados con la herramienta. Para ello se ubica en el icono  , aparecerá una nueva ventana que corresponde al **Asistente de Importación**, se debe marcar la opción **Microsoft Excel** y luego clic en el icono  , para

seleccionar el archivo que será analizado. Luego clic en **Siguiente** se accede al asistente de importación como lo muestra la Figura 3.17.

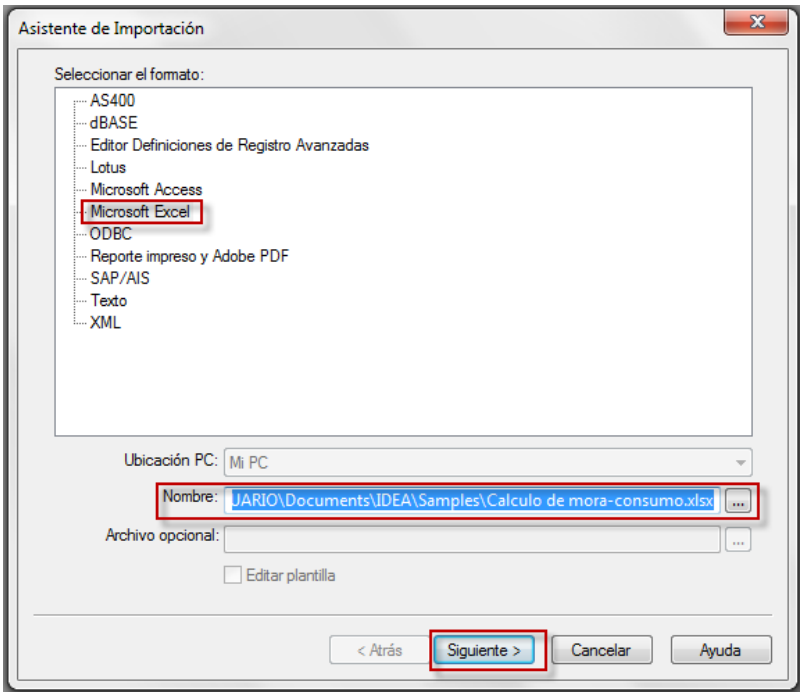


Figura 3.17. Asistente de importación

En la nueva ventana, seleccionar las dos opciones para que se muestren los encabezados correspondientes a cada campo del archivo de Excel y luego clic en **Aceptar**, como lo ilustra la Figura 3.18.

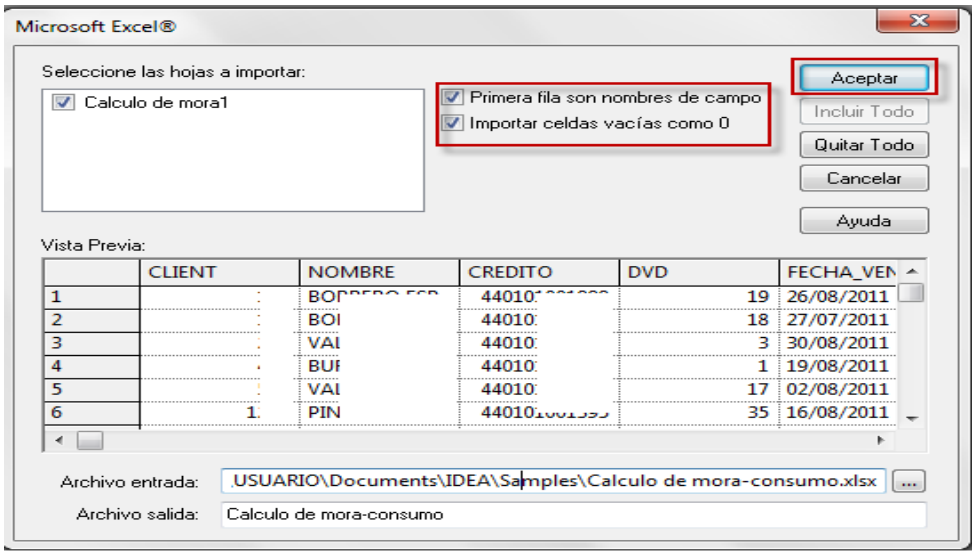


Figura 3.18. Importación de la base de datos

En la siguiente ventana como lo muestra Figura 3.19, aparecerá el archivo importado con la respectiva información.

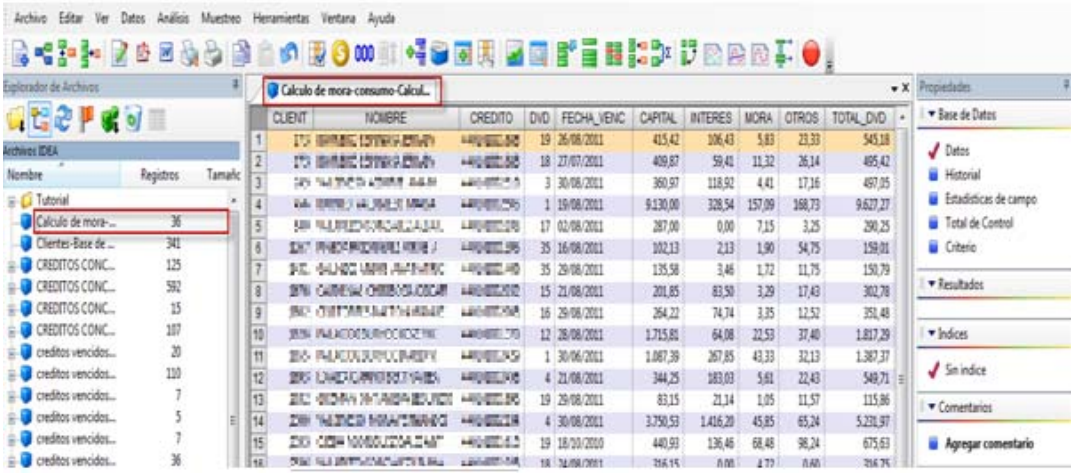


Figura 3.19. Archivo de importación

Seguidamente se procede a realizar las acciones necesarias en base a los criterios antes mencionados:

1. CONSISTENCIA DE INFORMACIÓN

- **Límite de créditos**

Con la finalidad de comprobar si los cupos de los créditos concedidos están acorde con lo reglamentado por la cooperativa, se aplica la opción extracción directa.

Para aplicar esta función se ha tomado como referencia los créditos concedidos (vigentes y cancelados) desde enero del 2004 hasta Septiembre del 2011, en sus diferentes tipos y montos como se muestra en la Tabla 3.4.

Tabla 3.4. Tipos de créditos

TIPOS DE CRÉDITOS	
CREDITO	**FINANCIA**
Comercial (desde $200 hasta 10% del patrimonio técnico de la cooperativa)	Capital de trabajo Comercio
Consumo (desde $200 hasta 10% del patrimonio técnico de la cooperativa)	Educación Salud Viajes Gastos varios
Vivienda (desde $200 hasta 10% del patrimonio técnico de la cooperativa)	Construcción de vivienda Adquisición de vivienda

Microcrédito (desde $200-5000)	Créditos a microempresarios Organización comunitaria[10]

En la Figura 3.20, se muestra la función **Extracción Directa** que será aplicada al reporte TotalCreditosConcedidos (Anexo 29) el cual está formado por listados de socios de todos los tipos de créditos, la cual permitirá obtener los montos de los créditos por cada socio, y de acuerdo a cada tipo de crédito.

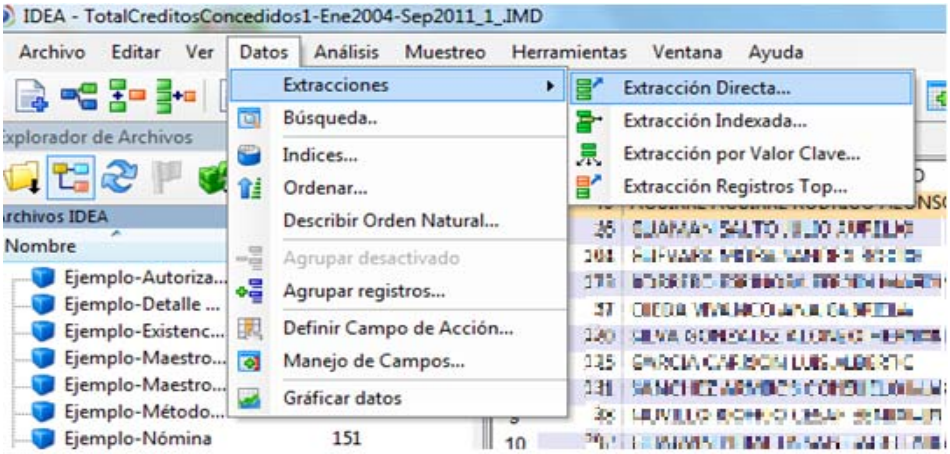


Figura 3.20. Opción Extracción Directa

En la Figura 3.21, se puede observar la formula MONTO > 80000.00, donde 80000.00 es el 10% del patrimonio actual de la cooperativa y es el valor máximo de crédito para los créditos de comercio y de consumo. Para microcrédito el MONTO >10000.00 en donde 10000.00 es el valor máximo de microcrédito según resolución emitida por el Consejo de Administración de la cooperativa, y para vivienda el MONTO > 40000.00, en donde 40000.00 es el valor máximo de créditos de vivienda según resolución emitida por el Consejo de Administración de la cooperativa.

[10] Fuente: Reglamento de Crédito de la Cooperativa de Ahorro y Crédito "Fortuna".

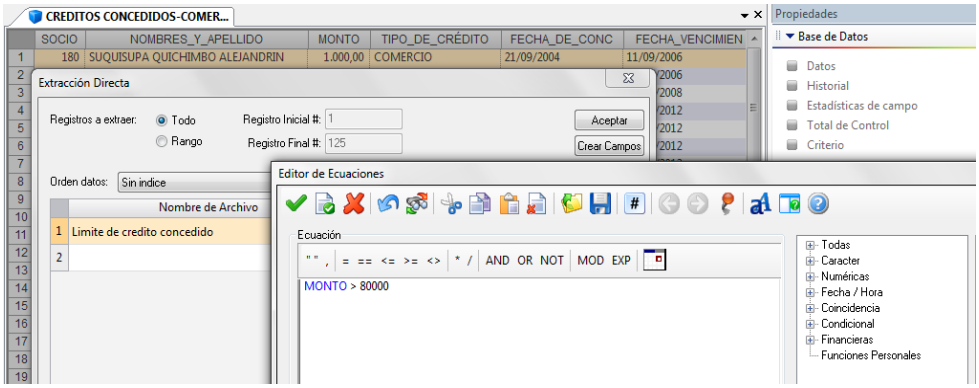


Figura 3.21. Fórmula para obtener el monto límite de Crédito Comercial y Consumo.

Como se muestra en la Figura 3.22, con extraccion directa se realiza la obtencion del límite de creditos concedidos en base al reporte TotalCréditosConcedidos el cual está formado por listados de socios de todos los tipos de créditos (Anexo 29).

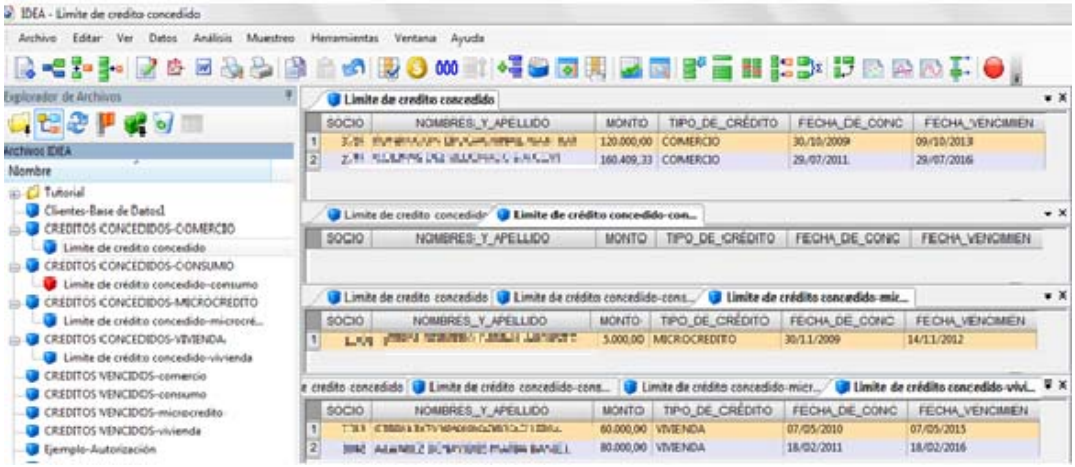


Figura 3.22. Resultados de límites elevados.

Luego de haber aplicado la formula correspondiente se ha obtenido los siguientes resultados:

- En crédito comercial, existen dos registros que exceden el monto mayor a 800000.00
- En crédito consumo, no existen registros, el icono se muestra en color rojo.
- En microcrédito, existe un registro que supera el monto mayor a 10000.00
- En crédito vivienda, existen dos registros que superan el monto mayor a 40000.00

En conclusión, con los resultados obtenidos se puede mencionar que no se ha cumplido con las políticas establecidas en el reglamento de crédito de la cooperativa ni con los cambios en los cupos de créditos emitidos por las resoluciones del Consejo de Administración, ya que los montos otorgados sobrepasan el límite estipulado.

- **Evaluar si los cálculos de intereses de mora son correctos**

Con la finalidad evaluar si los cálculos de intereses de mora coinciden con los cálculos que realiza el sistema informatico de la cooperativa, se aplica la opción comparar bases de datos.

Para aplicar esta función se ha tomado como muestra los créditos concedidos vigentes y vencidos desde Julio del 2010 hasta Septiembre del 2011, en sus diferentes tipos como se muestra en la Tabla 3.4.

En la Figura 3.23, se muestra la opción **Comparar Bases de Datos**, que será aplicada al reporte Créditos Vencidos el cual está formado por listados de socios de todos los tipos de créditos (Anexo 33).

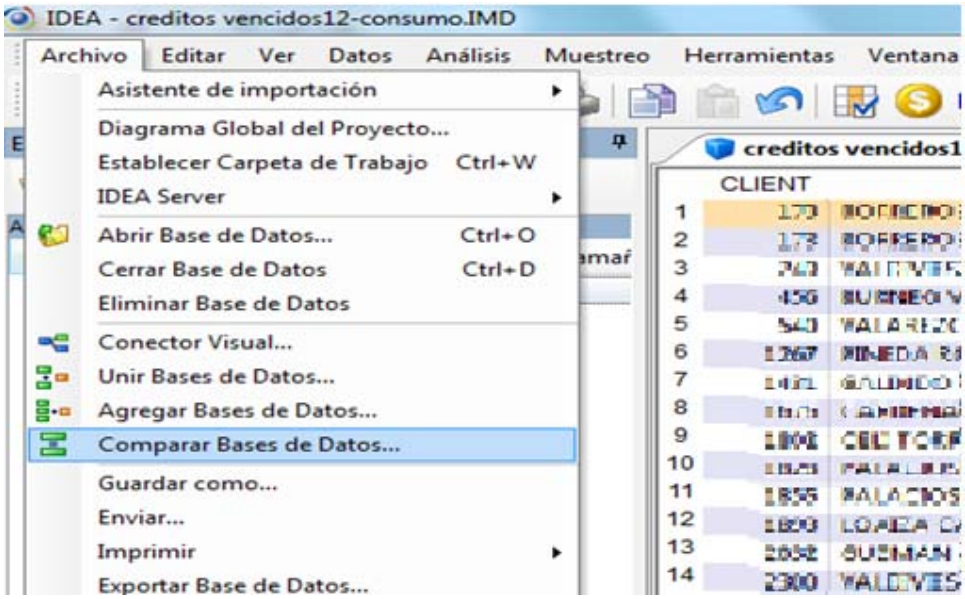


Figura 3.23. Opción Comparar Bases de Datos.

Primero se crea con IDEA una nueva base de datos por cada tipo de crédito con el nombre Cálculo de mora (Anexo 34), en esta base de datos que se calcula el campo MORA mediante una fórmula matemática, como se muestra en la Figura 3.24.

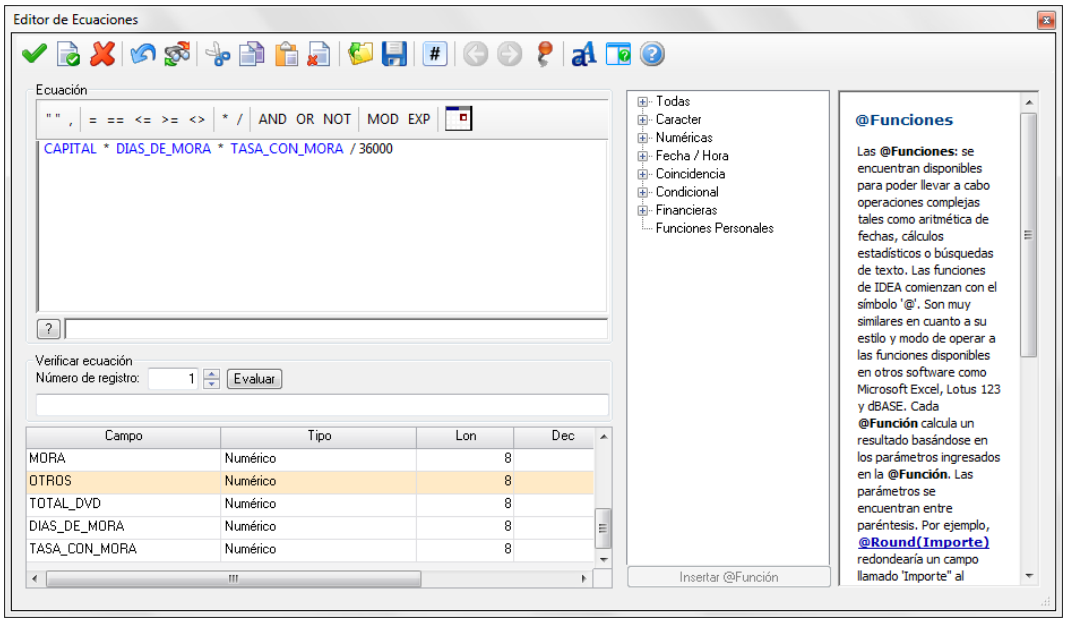


Figura 3.24. Calculo de mora en nueva base de datos.

Como se muestra en la Figura 3.25Figura 3.25, una vez que se tiene la nueva base de datos Cálculo de mora (Anexo 34) y con la base de datos del reporte Créditos Vencidos1 (Anexo 35), se realiza el proceso de comparación de las bases de datos en base al campo MORA con la función **Comparar Bases de Datos**, cuya coincidencia es el campo CLIENT.

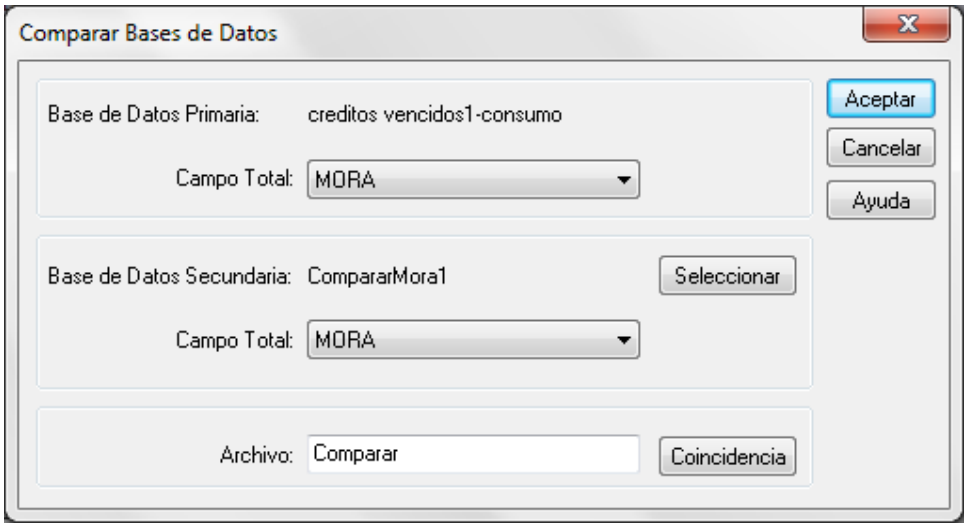


Figura 3.25. Proceso de comparación de dos bases de datos.

Los resultados de la comparación del campo MORA se muestran en la Figura 3.26, los campos TOTAL_P y TOTAL_S, son iguales, esto quiere decir que el cálculo de mora está correcto, con esto se comprueba que no hay ninguna diferencia en la mora en ninguno de los tipos de créditos otorgados, los resultados son los mismos en las dos bases de datos.

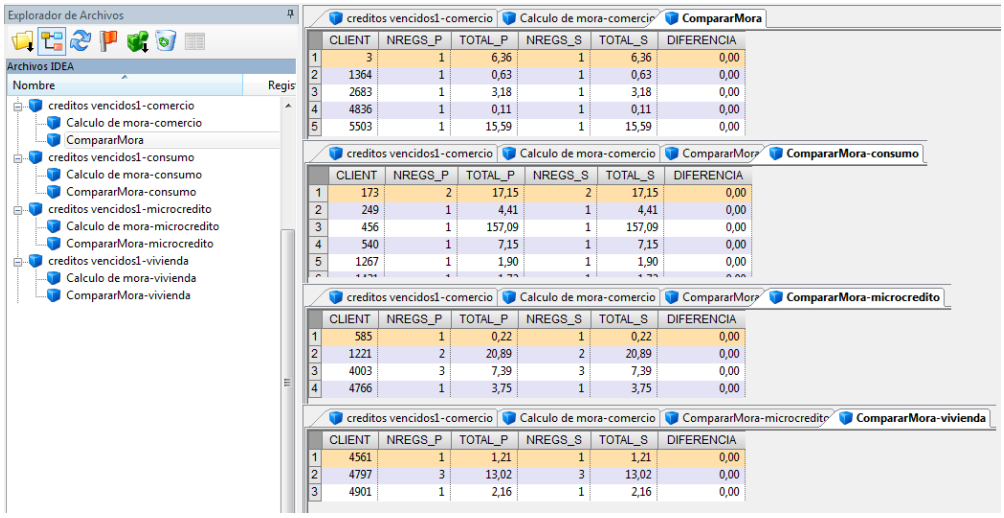


Figura 3.26. Resultados de la comparación del campo mora.

- **Totalizar las cuotas y días de mora por cliente para obtener los socios demandados**

Con la finalidad comprobar que los socios que tienen sus créditos vencidos más de noventa días están demandados, se aplica la opción sumarización.

Para aplicar esta función se ha tomado como muestra los créditos concedidos vigentes y vencidos desde Enero del 2005 hasta Septiembre del 2011, en sus diferentes tipos como se muestra en la Tabla 3.4.

En la Figura 3.27, se muestra la opción **Sumarización** que será aplicada al reporte créditos vencidos y demandados (Anexo 36), el cual está formado por listados de socios de todos los tipos de créditos, la cual permitirá obtener el total de los montos vencidos por cada socio, el total de dividendos vencidos el total de días de mora.

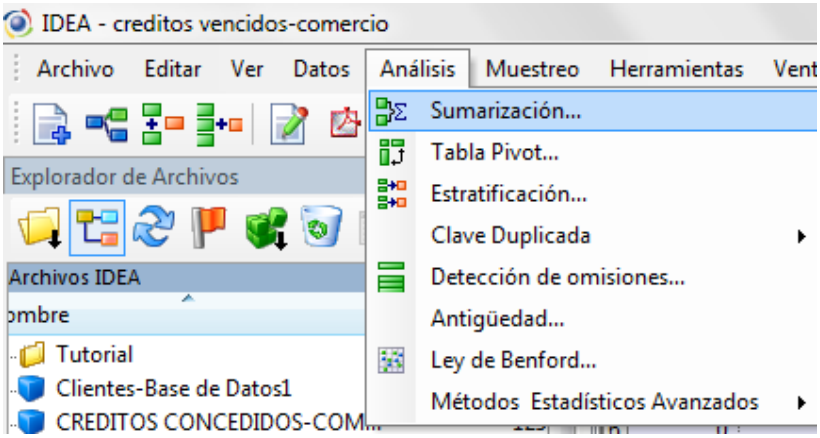


Figura 3.27. Opción Sumarización.

En la Figura 3.28, se realiza el proceso de **Sumarización** tomando el campo CLIENT**,** el campo TOTAL_DVD y el campo DIAS_DE_MORA**,** basado en el criterio DIAS_DE_MORA>=90, ya que los socios que estén vencidos más de noventa días deberían estar demandados**.**

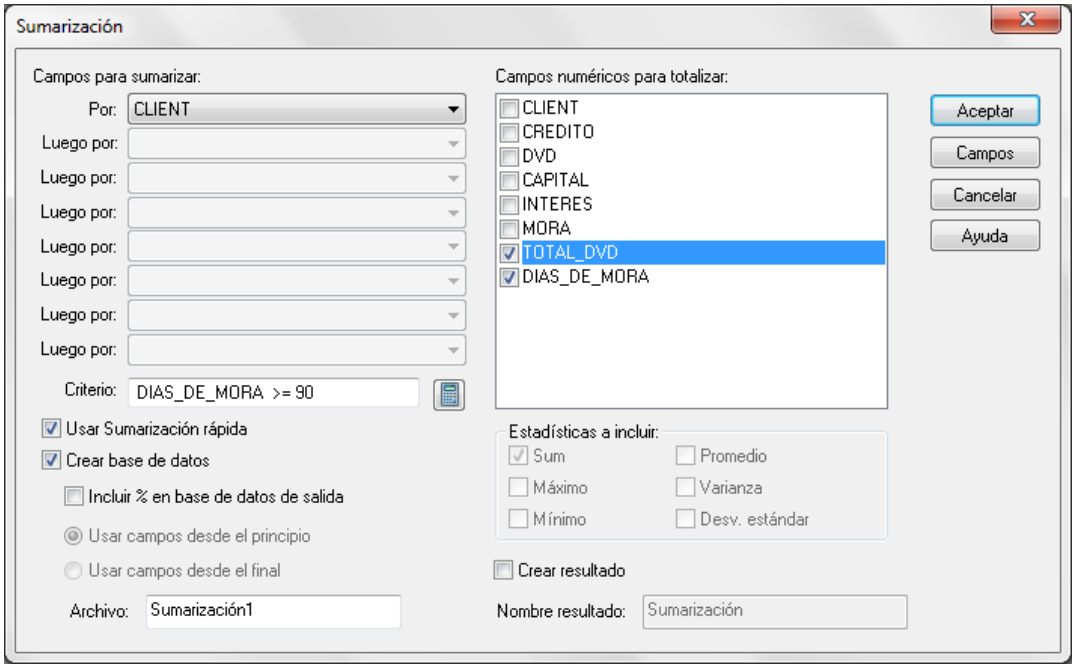


Figura 3.28. Proceso de Sumarización

Una vez aplicada la **Sumarización** a cada tipo de crédito, y como se puede observar en la Figura 3.29, existen socios con hasta veinte y un cuotas vencidas y con un valor de días de mora mayor a noventa, con estos resultados y con la observación de los reportes de créditos demandados (Anexo 10) que posee el departamento de crédito se pudo comprobar que los

socios que aparecen como resultado de la **Sumarización** efectivamente están demandados judicialmente por la cooperativa.

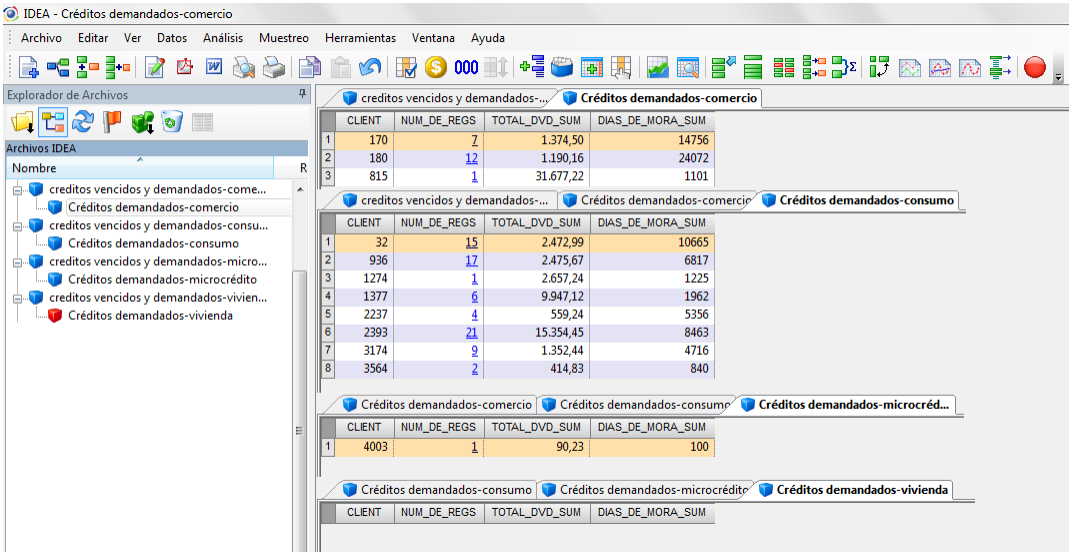


Figura 3.29. Resultados de clientes demandados.

2. REDUNDANCIA

- **Datos clave duplicados**

Con la finalidad comprobar que el número de crédito de un socio, en sus diferentes tipos de créditos, no sea el mismo número de crédito de otro socio, se aplica la **Clave Duplicada**.

Para aplicar esta función se ha tomado como referencia todos los créditos concedidos sean estos vigentes y cancelados (Anexo 37) desde Enero del 2004 hasta Septiembre del 2011, en sus diferentes tipos como se muestra en la Tabla 3.4.

En la Figura 3.30, se muestra la opción de **Clave Duplicada**, la cual permitirá realizar el proceso de verificación, para esto se utiliza el reporte TotalCreditosConcedidos (Anexo 29), que corresponde a todos los registros de los socios a quienes se les ha otorgado un crédito desde la apertura de la cooperativa.

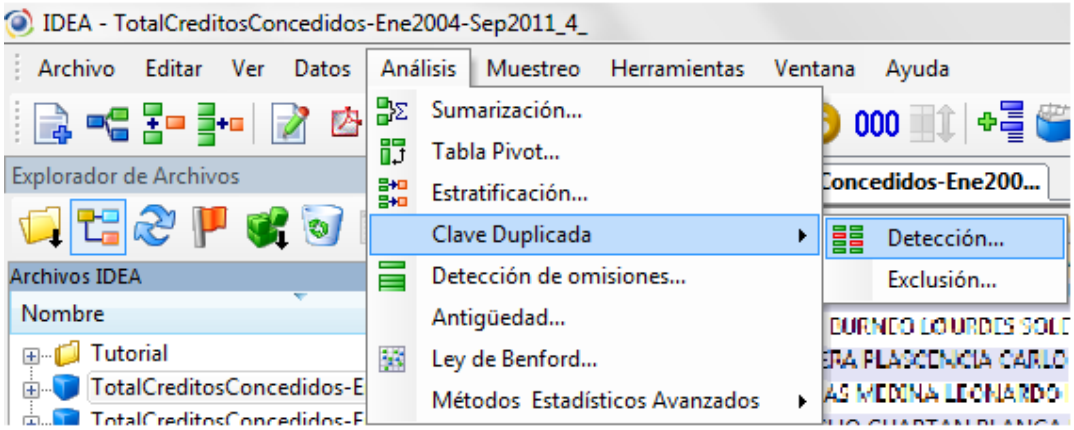


Figura 3.30. Opción Clave Duplicada.

Como muestra la Figura 3.31, luego de realizar la operación de verificación de **Clave Duplicada**, el símbolo en rojo indica que no existen valores repetidos, es decir que en todos los registros de créditos otorgados no existen números de créditos repetidos, por lo tanto ningún socio posee el mismo número de crédito de otro socio.

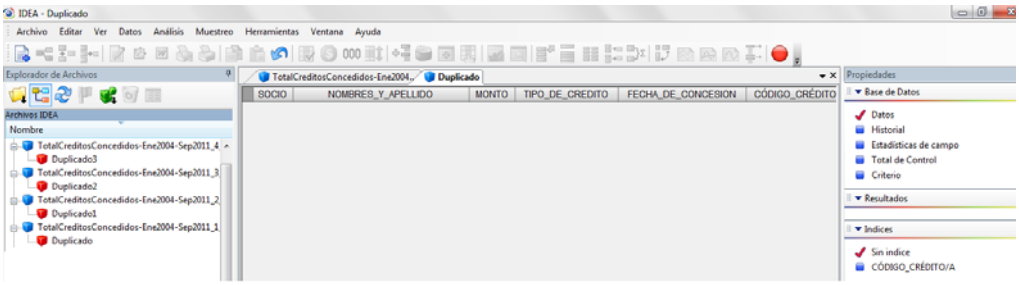


Figura 3.31. Resultado de la verificación de claves repetidas.

3. VALIDEZ

- **Verificar que no haya operaciones en fechas inusuales**

Con la finalidad de comprobar si se realizo algún desembolso de crédito en días no laborables en este caso día domingo, se aplica la opción **Extracción Directa**, como muestra la Figura 3.20.

Para aplicar esta función se ha tomado como referencia todos los créditos concedidos (vigentes y cancelados) desde Enero del 2004 hasta Septiembre del 2011, en sus diferentes tipos como se muestra en la Tabla 3.4.

La Figura 3.32, muestra la función y la fórmula para realizar una extracción, tomando como información los datos de del reporte TotalCréditosConcedidos (Anexo 29) para verificar si se ha realizado concesiones de créditos los días domingos,

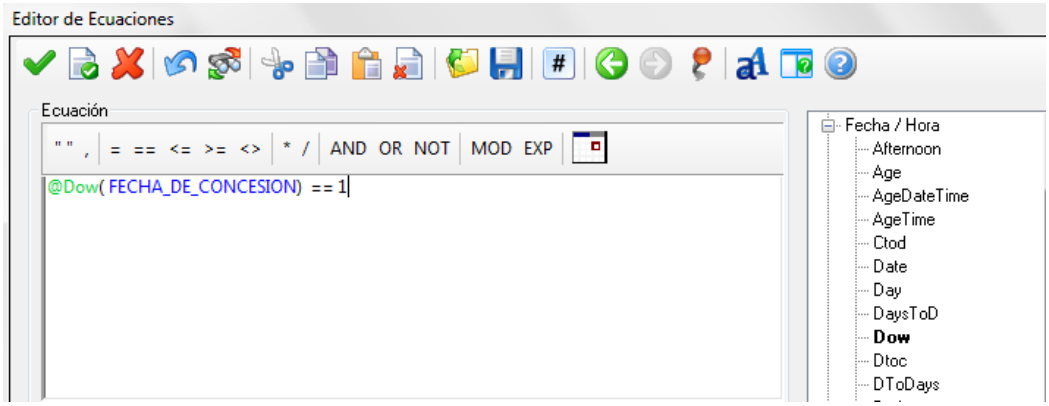


Figura 3.32. Fórmula para verificar operaciones el día domingo.

En la Figura 3.33, se realiza el proceso de extracción de datos, en la que se toma en cuenta el campo FECHA_DE_CONCES para ser analizado en base al criterio operaciones día domingo.

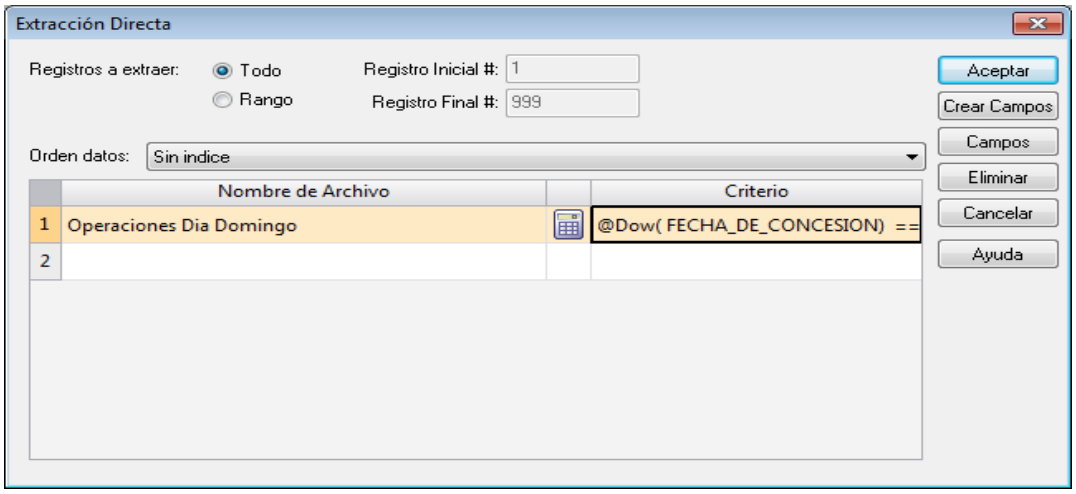


Figura 3.33. Extracción de datos dada la formula.

De acuerdo a los resultados que se muestran en la Figura 3.34, el icono en rojo indica que no existen registros para esta función, por lo tanto todas las fechas de concesión de crédito han sido realizadas en días laborables.

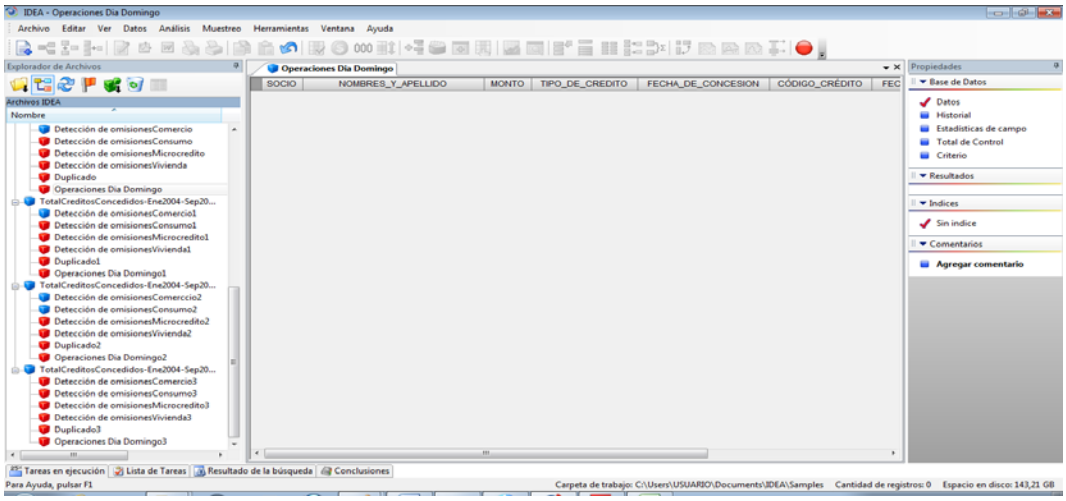


Figura 3.34. Resultados de operaciones en día Domingo.

4. INTEGRIDAD

- **Verificar que en las secuencias de los números de créditos no existan omisiones**

Con la finalidad de comprobar que los números de créditos, por cada tipo de crédito, mantienen una secuencia, se aplica la opción **Detección de Omisiones**.

Para aplicar esta función se ha tomado como referencia todos los créditos concedidos (vigentes y cancelados) desde Enero del 2004 hasta Septiembre del 2011, en sus diferentes tipos como se muestra en la Tabla 3.4.

Debido a que los tipos de crédito tienen códigos diferentes, ha sido necesario realizar la verificación de secuencias por cada tipo de crédito, para ello se han creado los siguientes comandos:

Campo a usar: CÓDIGO_CRÉDITO

Donde; TIPO_DE_CREDITO == "COMERCIO"

TIPO_DE_CREDITO == "CONSUMO"

TIPO_DE_CREDITO == "MICROCRE"

TIPO_DE_CREDITO == "VIVIENDA"

Cada tipo de crédito tiene su numeración, la cual está formada por el código asignado por defecto según el tipo de crédito y por la secuencia que se da conforme se van incrementando los créditos, así:

Créditos de COMERCIO 44010100……número según secuencia

Créditos de CONSUMO 44010200……número según secuencia

Créditos de VIVIENDA 44010300……número según secuencia

Créditos de MICROCREDITO 44010400……número según secuencia

En la Figura 3.35, se muestra la función de **Detección de Omisiones**, la cual permitirá realizar el proceso de comprobación, para esto se utiliza el reporte TotalCreditosConcedidos (Anexo 29), que corresponde a todos los registros de los socios a quienes se les ha otorgado un crédito desde la apertura de la cooperativa.

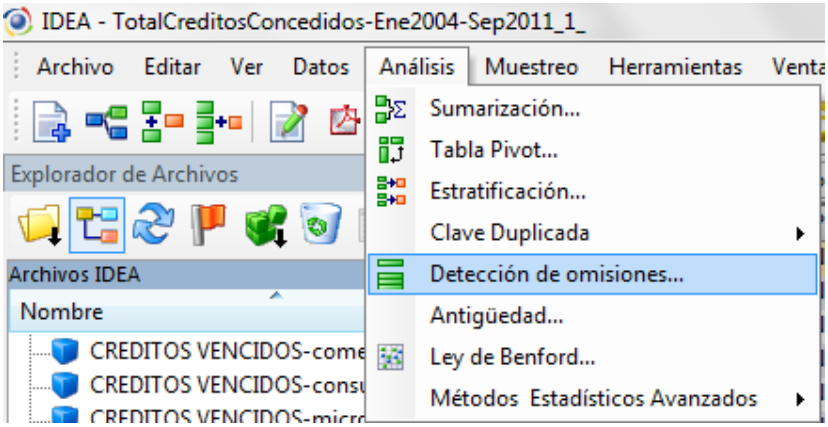


Figura 3.35. Opción Detección de Omisiones.

En la Figura 3.36, se realiza el proceso de **Detección de Omisiones**, en el que se toma en cuenta el campo CODIGO_CREDITO que es un identificador único, y será analizado en base al criterio TIPO_DE_CREDITO=="COMERCIAL" y por número de crédito,

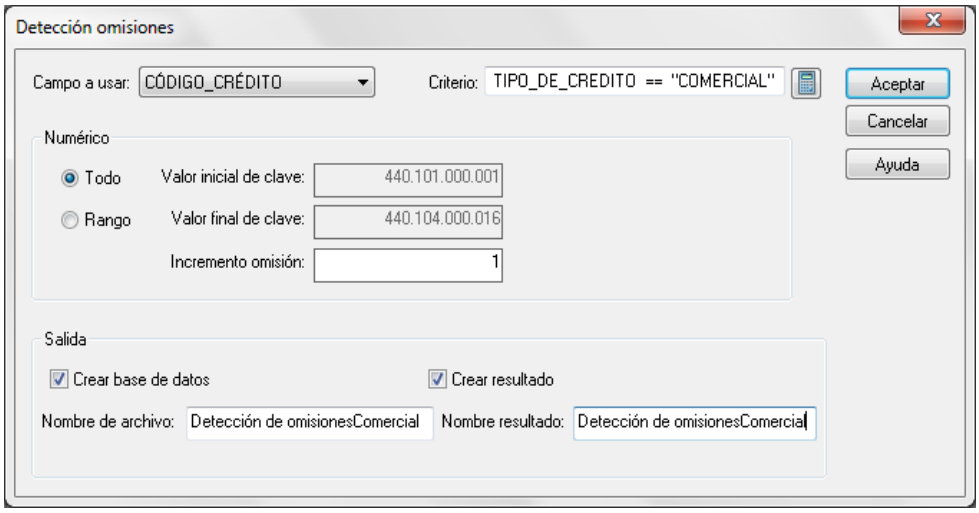


Figura 3.36. Proceso de detección de omisiones.

En la Figura 3.37, se obtienen los resultados de la ejecución de la opción **Detección Omisiones**, los reportes con icono en color azul dan como resultado que para el tipo de crédito de comercio existen seis omisiones en los registros, para el tipo de crédito consumo existen dos omisiones en los registros. Para el resto de tipos de crédito no existen omisiones como lo demuestra el icono de color rojo, por lo tanto no hay secuencias en la generación de los números de créditos.

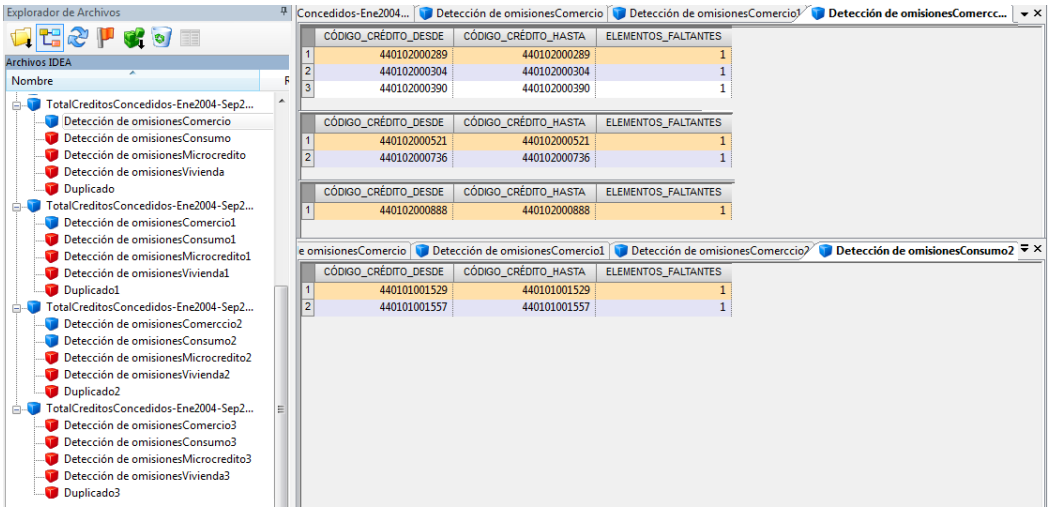


Figura 3.37. Resultados de detección de omisiones

RESULTADOS:

Finalmente de la aplicación de IDEA en base a los criterios de evaluación mencionados anteriormente, se puede concluir que:

- No se ha cumplido con las políticas establecidas en el reglamento de crédito de la cooperativa en cuanto a los montos establecidos para cada tipo de crédito, ya que existen créditos desembolsados con valores superiores a los fijados en dicho reglamento.
- El cálculo de mora que realiza el sistema con el que trabaja de la cooperativa es correcto.
- Los socios que están más de noventa días vencidos en los créditos, en efecto están demandados judicialmente por la cooperativa.
- No existen números de créditos repetidos, por lo tanto ningún socio posee el mismo número de crédito de otro socio.
- Todos los desembolsos de los créditos se han dado en días laborables.
- No hay secuencias en la generación de los números de créditos, existen ciertas omisiones.

3.3.3. APLICACIÓN DE LOS MODELOS DE MADUREZ

El modelo de madurez es una forma de medir qué tan bien están desarrollados los procesos administrativos de TI, con ello se determinarán procesos y sistemas críticos que requieren de una mayor atención que otros que son menos críticos.

Los modelos de madurez brindan un perfil genérico de las etapas a través de las cuales evoluciona la cooperativa para la administración y el control de los procesos de TI.

Los modelos de madurez COBIT no son un número al cual hay que llegar, ni están diseñados para ser una base formal de certificación, sin embargo, se diseñaron para ser aplicables siempre. En base a la escala de niveles de cada modelo de madurez, la administración de la cooperativa tendrá una idea clara de todo lo que engloba TI en la organización, y podrá catalogar, priorizar y establecer mejoras a los procesos de TI que se encuentran en niveles muy bajos permitiendo con su aplicación, mejorar el nivel de calificación y provocando con ello la perfeccionamiento continuo; siempre y cuando se tome en cuenta que existen algunos aspectos que dependen mucho tanto de recursos económicos , de recursos humanos y del tiempo.

3.4. VERIFICACIÓN DE EVIDENCIAS

En esta etapa mediante la técnica de la observación se pudo realizar la verificación de las evidencias y su respectiva localización, lo que permitió determinar el nivel de madurez en el que se encuentra la cooperativa en sus diferentes procesos de crédito.

El detalle de toda esta información encuentra en la matriz de evaluación (Anexo 22).

3.5. INFORME DE RESULTADOS

Luego del análisis de la información recopilada en base a los niveles de madurez, se presentan los siguientes cuadros resumen y la gráfica de dichos niveles en los cuales se encuentra la cooperativa por cada dominio de COBIT.

En base a la aplicación de la lista de chequeo que forma parte de la matriz de evaluación (Anexo 22) se pudo determinar que de los ocho procesos seleccionados, dos procesos se encuentran en la escala del nivel de madurez **uno** y seis procesos se encuentran en la escala del nivel de madurez **dos**.
A continuación en las siguientes tablas, se muestran los resultados del nivel de madurez actual obtenido por cada proceso COBIT.

Tabla 3.5. Nivel de Madurez del Dominio PLANEAR Y ORGANIZAR

DOMINIO	REF.	PROCESO	NIVEL DE MADUREZ
PLANEAR Y ORGANIZAR	PO6	Comunicar las Aspiraciones y la Dirección de la Gerencia	2 – REPETIBLE
	PO9	Evaluar y Administrar los Riesgos de TI	2 – REPETIBLE

Tabla 3.6. Nivel de Madurez del Dominio ADQUIRIR E IMPLEMENTAR

DOMINIO	REF.	PROCESO	NIVEL DE MADUREZ
ADQUIRIR E IMPLEMENTAR	AI4	Facilitar la Operación y el Uso	2 – REPETIBLE

Tabla 3.7. Nivel de Madurez del Dominio ENTREGAR Y DAR SOPORTE

DOMINIO	REF.	PROCESO	NIVEL DE MADUREZ
ENTREGAR Y DAR SOPORTE	DS4	Garantizar la Continuidad del Servicio	2 – REPETIBLE
	DS5	Garantizar la Seguridad de los Sistemas	2 – REPETIBLE
	DS11	Administrar los Datos	1 – INICIAL

Tabla 3.8. Nivel de Madurez del Dominio MONITOREAR Y EVALUAR

DOMINIO	REF.	PROCESO	NIVEL DE MADUREZ
MONITOREAR Y EVALUAR	ME2	Monitorear y Evaluar el Control Interno	1 – INICIAL
	ME3	Garantizar Cumplimiento Regulatorio	2 – REPETIBLE

La Figura 3.38, muestra la relación entre los niveles de madurez actuales de la cooperativa y los dominios COBIT que fueron seleccionados para esta auditoría.

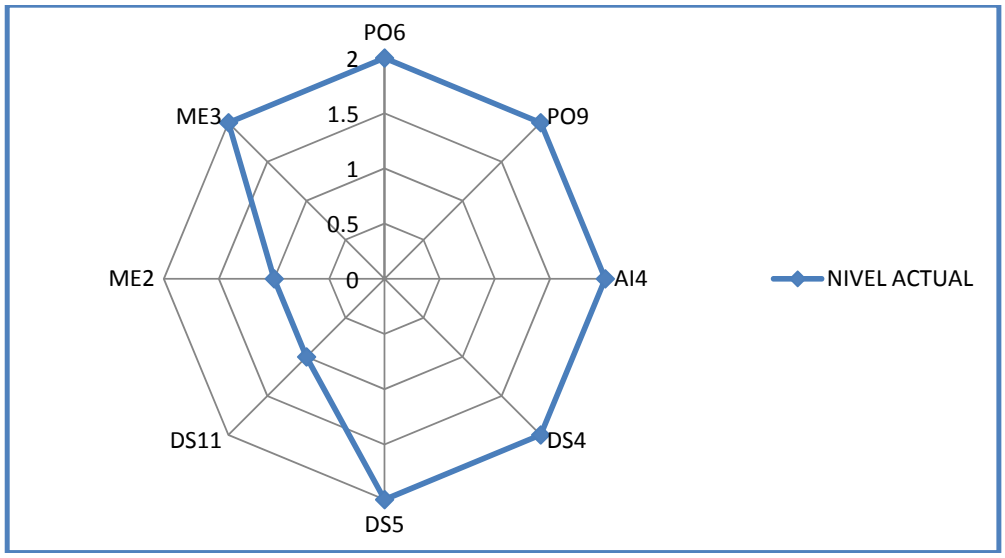


Figura 3.38. Comparativa de los niveles de madurez vs dominios COBIT.

3.5.1. HALLAZGOS DE LA AUDITORÍA

Una vez ejecutada la auditoría en la Cooperativa de Ahorro y Crédito "Fortuna", evaluando los niveles de madurez por cada dominio de COBIT, así como la aplicación de encuestas, la observación y la ejecución de las herramientas NESSUS e IDEA , se han detectado algunas falencias las cuales se detallan en una tabla de hallazgos.

Para poder comprender la tabla de hallazgos es necesario explicar de qué manera se determinó el nivel de criticidad en el que se encuentra cada descubrimiento, para ello se ha elaborado una matriz, la cual en base a ciertos criterios establece si el nivel de criticidad del hallazgo se encuentra en la escala alta, media o baja, todo esto se detalla en la Tabla 3.9.

Tabla 3.9. Matriz de Medición de Criticidad.

MATRIZ DE MEDICIÓN DE CRITICIDAD	
Nivel de Criticidad	**Criterio**
Alto	· Afecta a todos los departamentos de la cooperativa. · Incumplimiento con la mayoría de los objetivos de la cooperativa. · Potencial pérdida que afecta al patrimonio de la cooperativa. · Reclamos a gran escala de los usuarios de la cooperativa. · Afecta medianamente a la continuidad de la cooperativa.
Medio	. Afecta a la mayoría de departamentos de la cooperativa. · Incumplimiento con parte de los objetivos de la cooperativa. · Pérdida que afecta al patrimonio de la cooperativa. · Aumenta las quejas de los usuarios de la cooperativa. · Pone en peligro la continuidad de la cooperativa.
Bajo	· No afecta a ningún departamento de la cooperativa. · Incumplimiento en ningún objetivo de la cooperativa. · Mínimo impacto en el patrimonio de la cooperativa. · No existen quejas de los usuarios de la cooperativa. · No afecta a la continuidad de la cooperativa.

A continuación se presenta la tabla de hallazgos de la auditoría informática a la Cooperativa de Ahorro y Crédito "Fortuna" y su relación con cada proceso del COBIT.

Tabla 3.10. Hallazgos de la Auditoría Informática.

TABLA DE HALLAZGOS DE LA AUDITORÍA				
HALLAZGO	**NIVEL DE CRITICIDAD**	**ACCIONES RECOMENDADAS**	**PROCESO COBIT**	**PROCESO DE CRÉDITO**
Los manuales y reglamento de crédito no han sido actualizados desde el año 2009.	Bajo	Actualizar el reglamento de crédito.	PO6	PC1, PC2, PC3
No existe un manual de procedimientos para gestión interna.	Bajo	Definir manual de procedimientos para gestión interna.		
No se cumple con el cronograma establecido para capacitación al personal en cuanto a políticas.	Bajo	Definir un cronograma para capacitación al personal.		

Existen créditos otorgados cuyos montos por tipo de crédito superan lo establecido en el reglamento de crédito.	Alto	Revisión de las políticas del reglamento de crédito.		
No existen políticas de seguridad de TI.	Medio	Implementar políticas de seguridad de TI.		
No existe un marco de trabajo para evaluación de riesgos.	Medio	Definir un marco de trabajo.	PO9	PC1, PC2, PC3, PC4, PC5
No existe un plan de acción documentado contra riesgos crediticios, tecnológicos, de seguridad, de continuidad.	Medio	Definir y documentar un plan de acción de riesgos.		
No está definida la evaluación y administración de riesgos en TI (amenazas, vulnerabilidades).	Medio	Definir, documentar y comunicar la administración de riesgos de TI.		
No existe evidencia de que se haya definido y comunicado el grado de tolerancia del riesgo en TI.	Medio	Definir, documentar y comunicar la administración de riesgos de TI.		
Existen vulnerabilidades tanto en los servidores como en las terminales de crédito.	Alto	Actualizar el sistema operativo Windows 2000 o cambiarse a un sistema operativo menos vulnerable.		
No se cuenta con un plan general para cubrir las necesidades referentes a la elaboración de las aplicaciones informáticas que desarrolla el departamento de sistemas de la cooperativa.	Medio	Establecer una adecuada planificación para el desarrollo y la adquisición de aplicaciones de acuerdo a los requerimientos de la cooperativa.	AI4	PC4, PC5
Los manuales de usuario del aplicativo con el que trabaja la cooperativa son obsoletos	Medio	Actualizar los manuales de usuario.		
No se da capacitación a los usuarios del sistema financiero con el que opera la cooperativa, por parte de los proveedores del mismo.	Medio	Establecer acuerdos firmados de capacitación al personal para uso del sistema.		
No existe un plan de contingencias	Alto	Elaboración de un plan de contingencias debidamente documentado y aprobado. Revisar y actualizar periódicamente las políticas del plan de contingencias.	DS4	PC4, PC5

No existe la debida seguridad física en el centro de cómputo.	Alto	Implementación de seguridad física e infraestructura.		
Falta de actividades definidas para la administración de riesgos crediticios, tecnológicos, de seguridad, de continuidad.	Alto	Definir actividades para la administración de riesgos (riesgos crediticios, tecnológicos, de seguridad, de continuidad).	DS5	PC4, PC5
No se presta atención a la seguridad de TI a nivel de software ni de hardware.	Alto	Concienciar y capacitar a todo el personal de la cooperativa a cerca de la importancia de la seguridad tanto a nivel de software como de hardware.		
No existen políticas y procedimientos estandarizados de seguridad de TI.	Alto	Implementar políticas y procedimientos de seguridad estandarizados, revisar y confirmar periódicamente los derechos de acceso, riesgo de errores, fraudes, alteración no autorizada o accidental.		
No existen seguridades en la red y el antivirus con el que cuenta la cooperativa no brinda la confianza necesaria.	Alto	Implementar las soluciones propuestas por la herramienta NESSUS para mitigar las vulnerabilidades existentes. Implementar un adecuado control de virus informático en los equipos.		
A la información física de los créditos tiene acceso cualquier empleado de la cooperativa.	Alto	Restringir a usuarios no autorizados el acceso a información confidencial de los socios implementando técnicas de seguridad.		
No existe evidencia de procedimientos para establecer revisiones periódicas de los derechos de acceso asignados a los usuarios del aplicativo con el que opera la cooperativa.	Alto	Contratar los servicios de un especialista de seguridad para la identificación de amenazas.		

No está documentado un procedimiento que permita eliminar los respaldos de la información de manera segura cuando estos ya no se los utilice o hayan cumplido con el tiempo de permanencia.	Medio	Definición de un procedimiento para la eliminación de respaldos dentro de las políticas del departamento de sistemas.	DS11	PC4, PC5
No existe seguridad con la información física de los socios de crédito.	Alto	Establecer mecanismos de seguridad para la documentación de los socios.		
No se cuenta con un inventario de los recursos críticos de software y hardware de la cooperativa.	Alto	Implementar procedimientos para mantener un inventario de los recursos críticos de software y hardware.		
Los montos de créditos según el tipo de préstamo no están parametrizados en el sistema con el que opera la cooperativa.	Alto	Parametrizar en el sistema de la cooperativa los montos de créditos, según su tipo.		
En el tipo de créditos de comercio y créditos de consumo existen omisiones en las secuencias de los números de crédito.	Medio	Implementación de controles en el sistema.		
Falta de estándares de representación de datos.	Alto	Implementar estándares de representación de datos.		
No existe un programa de control interno y proceso de monitoreo de TI.	Medio	Definir y documentar un programa de monitoreo y control interno de TI.	ME2	PC1, PC2, PC3, PC4, PC5
Falta de seguimiento y evaluación de procesos de TI.	Medio	Contratar los servicios profesionales de un auditor informático.		
No se hacen revisiones de auditoría interna al departamento de sistemas.	Alto	Realizar auditoría al departamento de sistemas.		
No se dan procesos de evaluación de tecnología de información.	Alto	Definir y documentar un programa de evaluación de TI.	ME3	PC1, PC2, PC3, PC4,
La cooperativa no cuenta con un comité de seguridad informática.	Medio	Conformar un comité de seguridad informática.		

No se garantiza que los requisitos legales y regulatorios se cubran y cumplan de forma eficiente.	Medio	Contratación de servicios profesionales para el área de seguridad informática con el fin de garantizar que los requisitos legales y regulatorios del departamento de sistemas se cubran y cumplan de forma eficiente.		PC5

CAPÍTULO 4:

RESULTADOS DE LA AUDITORÍA INFORMÁTICA

4. *RESULTADOS DE LA AUDITORÍA INFORMÁTICA*

En esta fase se presentan los resultados de la auditoría realizada a la Cooperativa de Ahorro y Crédito "Fortuna", los cuales permite evaluar el control del departamento de crédito, medir la eficacia del sistema informático, verificar el cumplimiento de la normativa de los organismos de control y revisar la gestión de los recursos de TI.

En esta sección también se plantean una estrategia para resolver las criticidades encontradas y se realiza el Plan de acción a partir de los hallazgos de la auditoría informática, los cuales se obtuvieron mediante la aplicación de los modelos de madurez y las herramientas IDEA y NESSUS.

Finalmente se define un plan de acción con actividades que ayuden tanto a Gerencia General como al Consejo de Administración en la toma de decisiones para mejorar los procesos en la cooperativa "Fortuna".

Cabe mencionar que cada proceso de COBIT cuenta con un conjunto de mejores prácticas para la seguridad, calidad, eficacia y eficiencia en TI, las cuales sirven como pautas para alinear TI con las actividades de la cooperativa, identificar riesgos, gestionar recursos y medir el desempeño y cumplimiento de metas y evaluar el nivel de madurez de los procesos de la entidad.

4.1. ANÁLISIS DE RESULTADOS

Una vez finalizada la auditoría informática a la Cooperativa de Ahorro y Crédito "Fortuna", se han podido determinar algunas fortalezas y debilidades existentes, a las cuales se las detalla a modo de causa y efecto en las siguientes tablas:

FORTALEZAS

Tabla 4.1. Fortalezas encontradas luego de realizada la Auditoría Informática.

EFECTO	CAUSA
La cooperativa cuenta con un reglamento de crédito.	Existe un Consejo de Vigilancia, los cuales se reúnen semanalmente y controlan el cumplimiento de las políticas de crédito.
Se lleva un control manual y sistemático de los créditos al día y de los créditos vencidos y no pagados.	Existe monitoreo por parte de la Gerencia de la recuperación de los créditos.
Controles de auditoría interna	La cooperativa ha reconocido que los problemas de control interno existen y que necesitan ser resueltos. Se hacen revisiones de auditoría interna al departamento de crédito, en base a las políticas, leyes y regulaciones de la cooperativa. Auditoría interna y los miembros del Consejo de

	Vigilancia se encargan de verificar el cumplimiento regulatorio en cuanto a los créditos otorgados. Auditoría interna realiza revisiones periódicas de los créditos. El Consejo de Vigilancia se reúne semanalmente para realizar las revisiones de los créditos otorgados, vigentes, vencidos y demandados, en el caso de que en los informes del Consejo de Vigilancia o de auditoría Interna se notifiquen errores estos deben ser corregidos a la brevedad del caso. Existe un documento firmado por el personal de crédito en el cual se determina la confidencialidad y el sigilo. Los contratos de préstamos y pagarés de crédito son redactados por el asesor legal de la cooperativa, por lo tanto son documentos que respaldan legalmente las operaciones de crédito.
Seguridades de ingreso	El aplicativo con el que opera la cooperativa bloquea al usuario cuando se han dado tres intentos de ingresos con claves inválidas El sistema con el que opera la cooperativa posee expiración mensual de claves.
Adecuado procesamiento de datos.	El aplicativo con el que opera la cooperativa provee de una adecuada automatización de los desembolsos y recuperación de los créditos. El cálculo de los intereses normales e intereses de mora que realiza el sistemas a los diferentes tipos de crédito son los correctos. Los números de crédito de un socio, en sus diferentes tipos de préstamos, no es el mismo número de crédito de otro socio, es decir no se dan duplicidades de los números de créditos.
La continuidad del servicio se cumple por responsabilidad del departamento de sistemas.	Seguridad en el resguardo de información de la base de datos. Existen mecanismos para reanudación de servicios en caso de cortes de energía o falencias en los servidores. Las bases de datos son respaldadas a diario en cd´s reutilizables y cada cuatro meses estas son reemplazadas por nuevos respaldos, el resguardo de los cd´s se lo realiza fuera de las instalaciones

	de la cooperativa. Existe un inventario del almacenamiento de los cd´s de respaldos de las bases de datos.
Control de tráfico de internet	La cooperativa cuenta con un firewall el cual impide que software malintencionado o usuarios no autorizados puedan tener acceso a los equipos a través de internet o de la red, además permite filtrar los correos basura.

DEBILIDADES

Las debilidades se han clasificado por el objeto de análisis así:

1) POLÍTICAS Y PROCEDIMIENTOS

Tabla 4.2.Debilidades en cuanto a políticas y procedimientos luego de realizada la Auditoría Informática.

EFECTO O PROBLEMA	CAUSA
El cumplimiento de las políticas de crédito no es riguroso.	Manuales y reglamentos de crédito no están actualizados. Cambios frecuentes a las políticas de crédito. No se capacita a los empleados en la aplicación de las políticas. Alto grado de confianza en los conocimientos de los empleados. Falta de procedimientos para monitorear si el personal de la cooperativa ha comprendido y cumplido la normatividad institucional.
No existen políticas referentes a TI.	Falta de control en la seguridad, confidencialidad y controles internos. Falta de recursos para implantación de estas políticas. Se desconoce la responsabilidad acerca de la difusión de las políticas. No se tienen objetivos de TI orientados hacia la calidad. Ausencia de una persona que realice auditoría informática lo cual no le permite obtener un aseguramiento efectivo de los controles internos de TI.

	Falta de auditorías internas al departamento de sistemas. Falta de evaluación a los procesos de TI. Falta de controles que permitan evaluar la gestión de TI.
No existen políticas y procedimientos estandarizados de seguridad.	No se identifican los requerimientos de seguridad aplicables al recibo, procesamiento, almacenamiento y salida de los datos. Ausencia de un comité de seguridad informática.

2) SEGURIDAD FÍSICA

Tabla 4.3.Debilidades en cuanto a seguridad física luego de realizada la Auditoría Informática.

EFECTO O PROBLEMA	CAUSA
No existe un plan de contingencias documentado ni aprobado para poder evaluar y minimizar interrupciones de los servicios prestados de TI.	No hay la debida seguridad física en el cuarto en donde están los servidores, y no está organizado como debe ser. La cooperativa no ve la seguridad de TI tanto a nivel de software como de hardware como parte de su propia disciplina. La seguridad de TI es limitada. Falta de una evaluación de riesgos de fallas o interrupciones. Falta de procedimientos para mantener el inventario de los recursos críticos de software y hardware de la cooperativa. No existe evidencia de un procedimiento para mantener el inventario de los recursos críticos de software y hardware de la cooperativa. Falta de controles que permitan evaluar la infraestructura de redes y las comunicaciones.
A la información crediticia tiene acceso cualquier empleado de la cooperativa.	Escasa seguridad en los lugares de almacenamiento de las carpetas de los socios de crédito. Espacio físico pequeño.
Falta de un plan de acción documentado contra Riesgos.	No existe un proceso para la Evaluación e Identificación de Riesgos del negocio, ni un marco de referencia relacionado.

	No se da un enfoque general para la evaluación de riesgos (alcance, límites, metodología, responsabilidades y habilidades). No se han implementado estrategias para evitar riesgos crediticios.
Falta de definición en la evaluación y la administración de riesgos de TI.	No se identifican todos los eventos, sean estos amenazas o vulnerabilidades. No se determinan el nivel de impacto de los riesgos en la cooperativa, por lo que ello puede afectar considerablemente a los activos de la información de la institución. Monitoreo del desempeño de TI de manera informal. No se ha definido y comunicado el grado de tolerancia de riesgos de TI.

3) SISTEMA

Tabla 4.4.Debilidades en cuanto al sistema luego de realizada la Auditoría Informática

EFECTO O PROBLEMA	CAUSA
El sistema informático de la cooperativa ya ha terminado su ciclo de vida dentro de la misma.	Falta de procedimientos para asegurar acciones oportunas relacionadas con la solicitud, establecimiento, emisión, suspensión y cierre de cuentas de usuario del sistema. Ya no se adapta a las necesidades del negocio actual y futuro por lo que se deben realizar muchos procesos de forma manual lo que retrasa la ejecución de procesos y genera cuellos de botella en algunos departamentos. La estructura de la base de datos y el motor de la base están desactualizados. Creación de pequeñas aplicaciones extras de acuerdo a las necesidades de la cooperativa, éstos programas son probados por los usuarios de la cooperativa antes de su aplicación, para la elaboración de estos programas no hay un plan general para dar entrenamiento, la capacitación a estos programas se da de manera informal, y la responsabilidad en estos se deja al usuario, por lo tanto es probable que se generen errores.

Escasa capacitación en el uso del sistema informático de la cooperativa.	Falta de conocimiento sobre la existencia de tablas de claves de usuario. Desconocimiento sobre la encriptación de las claves de usuario. Los proveedores del sistema no brindan de manera efectiva ni eficiente el apoyo que se requiere en cuanto a las falencias del mismo. Los manuales del aplicativo son obsoletos.
El sistema informático es vulnerable.	No posee configuraciones de registro. Falta de procedimientos para establecer revisiones periódicas de los derechos de acceso asignados los usuarios del sistema. El sistema no tiene parametrizados los montos de créditos según el tipo de crédito. Omisiones en las secuencias de la numeración de los créditos desembolsados.

4) SERVIDORES

Tabla 4.5.Debilidades en cuanto a servidores luego de realizada la Auditoría Informática

EFECTO O PROBLEMA	CAUSA
Servidor de usuario Windows 2000 Service Pack 4.	Sistema operativo obsoleto. No tiene soporte para las vulnerabilidades existentes. Falla en la interfaz RPC (Llamada a Procedimiento Remoto) Falla en la función RemoteActivation. Es posible obtener el SID (identificador único para la sesión de usuario) del servidor, sin credenciales. Se puede acceder a un recurso compartido de red usando una sesión nula permitiendo a un atacante leer o escribir los datos confidenciales. Interrupciones en los servicios informáticos causadas por virus. Permite logins con texto claro permitiendo a los atacantes manejar usuarios y contraseñas por sniffing de tráfico al servidor.

	Los host tienen contraseñas configuradas para que nunca expiren. Los controles de seguridad local están desactivados. Es posible logearse en el equipo con una sesión NULL (sin login y password) No soporta nuevas bases de datos. No soporta nuevas aplicaciones.
Servidor de BD con sistema operativo LINUX CENTOS 5.2.	Poca compatibilidad para importar desde Windows. Instalar controladores de hardware y programas resulta complicado. No soporta aplicaciones tipo web.
Motor de base de datos INFORMIX	Lentitud en el procesamiento de peticiones múltiples. Pocas aplicaciones de tipo financiera trabajan con este gestor de BD. No brinda seguridades.
Equipo obsoleto	Baja capacidad de almacenamiento. Su vida útil caduca en mayo del 2012. 2GB memoria RAM del servidor de BD. 2.66 GHz procesador del servidor de BD. 1GB memoria RAM del servidor de usuarios. 2.86 GHz procesador del servidor de usuarios. 80 GB memoria del disco duro del servidor de usuario y de BD .

4.2. DEFINICIÓN DE OPORTUNIDADES DE MEJORA

Con la finalidad de mejorar la calidad del servicio en la cooperativa y optimizar e incrementar las seguridades, tanto a la red de datos como a la base de datos del sistema, se presenta una propuesta económica, técnica y operativa que podrá dar solución a varios inconvenientes con los actuales servidores.

Se plantea el cambio de los servidores existentes por servidores virtualizados tipo rack, y para ello se ha tomado en consideración que la cooperativa debería contar con:

- Un servidor para la aplicación.
- Un servidor de correo y página web propios ya que actualmente tienen contratado un Hosting, y por motivos de seguridad lo ideal sería tener una página web local para poder implementar una web transaccional.

- Un servidor proxy para control de tráfico de internet, ya que actualmente es el firewall el encargado de esto.
- Un servidor de directorio activo para control de la red de local.
- Un servidor de antivirus.

A continuación se detalla el análisis económico, técnico y operativo de los equipos y software a usarse.

Propuesta Técnica:
Los recursos requeridos para la puesta en marcha del proyecto serian básicamente los siguientes:

- Servidor de base de datos tipo torre.
- Software y licencias
- UPS.

Propuesta Económica [64]:
En cuanto a los costos de recursos de hardware y software a adquirir, se han tomado en cuenta los siguientes:

Tabla 4.6.Propuesta Económica de Dispositivos.

DISPOSITIVOS	CANTIDAD	PRECIO	SUBTOTAL
Rack cerrado	1	900.00	900.00
Servidor para rack	1	3158.00	3158.00
UPS de rack de 6 kva	1	1050.00	1050.00
Switch de 24 puertos administrable	1	405.00	405.00
Patch panel de 24 puertos para rack de 19"	1	50.00	50.00
Patch cord de 1 metro	19	2.00	38.00
		Total (USD)	**4208.00**

Tabla 4.7.Propuesta Económica de Software.

SOFTWARE/ LICENCIA	CANTIDAD	PRECIO	SUBTOTAL
Sistema Operativo para Servidor	1	2400.00	2400.00
Software Antivirus	19	45.00	855.00
Software Base de Datos	1	5400.00	5400.00
Licencia de Core Cal para acceso a base de datos y domino	19	150.00	2850.00
		Total (USD)	**11505.00**

El total de la inversión para implementar los servidores virtualizados sería de $15713.00

Cabe mencionar que los servidores virtualizados tienen mucha ventaja, ya que su respaldo es más fácil y se lo puede migrar sencillamente, además consumen menos energía lo que ahorraría gastos a la cooperativa.

Propuesta Operativa:
Los requisitos óptimos que se han considerado para esta alternativa se listan en el Anexo 32.

4.3. PLAN DE ACCIÓN

Después de haberse establecido los hallazgos de la auditoría informática realizada mediante la aplicación de los modelos de madurez del marco referencial COBIT y las herramientas IDEA y NESSUS, se plantean las siguientes recomendaciones, con el responsable de ejecutarlas, los tiempos estimados para su cumplimiento y los costos aproximados.

En el plan de acción es necesario priorizar la urgencia con las que se deben resolver los problemas encontrados en la auditoría, es por ello que es conveniente realizar algunas actividades en paralelo. El detalle de todas y cada una de las actividades se muestra en el cronograma que se muestra en la Figura 4.1.

Id	Nombre de tarea	Duración
1	IMPLEMENTACIÓN DEL PLAN DE ACCIÓN	153 días?
2	Definir políticas de seguridad, confidencialidad y procesos internos.	30 días
3	Revisión, aprobación y difusión de las políticas de seguridad, confidencialidad y procesos internos.	30 días
4	Definición de un plan de acción documentado y formal para evaluación de riesgos crediticios.	30 días
5	Revisión, aprobación y difusión del plan de acción para evaluación de riesgos crediticios.	30 días
6	Definición de un plan de acción documentado y formal para evaluación de riesgos de TI.	30 días
7	Revisión, aprobación y difusión del plan de acción para evaluación de riesgos de TI.	30 días
8	Implementar la gestión de riegos de TI.	30 días
9	Actualizar el sistema operativo de los servidores a Microsoft Windows Server 2008 R2 Standard w/SP1.	15 días
10	Actualizar el sistema operativo de las terminales de la cooperativa por el MS OEM Windows 7 Profesional SP1.	15 días
11	Elaboración de un plan de contingencia	60 días
12	Revisión, aprobación y difusión del plan de contingencias	30 días
13	Implementar el plan de contingencias	30 días
14	Resolver los problemas de seguridad de la red, derechos de acceso, riesgo de errores, fraudes, alteración no autoriza	30 días
15	Adquirir un antivirus para los dos servidores, recomendable Enterprise Security for Endpoints - Server Protect de la m	15 días
16	Adquirir un antivirus para las catorce terminales por Enterprise Security for Endpoints- Ofiice Scan de la marca Trend I	15 días
17	Adquirir mecanismos de seguridad para restringir a personal no autorizado el acceso a la información física de los soci	15 días
18	Adquirir un nuevo software financiero de acuerdo a los requerimientos de la Cooperativa y capacitar al personal en su	120 días
19	Actualizar y difundir el reglamento de crédito.	30 días
20	Formular un manual de procedimientos de gestión interna para el departamento de crédito.	60 días
21	Revisión, aprobación y difusión del manual de procedimientos de gestión interna para el departamento de crédito.	30 días
22	Elaborar un reglamento para el departamento de sistemas.	60 días
23	Revisión, aprobación y difusión del reglamento para el departamento de sistemas.	30 días
24	Implementar un proceso de seguimiento y control de las acciones de cobranza de la cartera de crédito.	30 días
25	Automatizar la elaboración del informe de crédito y del pagaré de crédito.	15 días
26	Capacitar al personal, para de esta manera evitar posibles errores o riesgos que puedan producirse en los procesos o a	15 días
27	Incorporar eventos de simulacro dentro del entrenamiento de la contingencia para una respuesta a la verificación efe	30 días
28	Concienciar y capacitar a todo el personal de la cooperativa acerca de la importancia de la seguridad tanto a nivel de s	30 días
29	Estructurar un inventario de los recursos críticos de software y hardware de la Cooperativa.	30 días
30	Definir, documentar y difundir un programa de monitoreo y control interno para el área de crédito.	30 días
31	Definir, documentar y difundir un programa de monitoreo y control interno para el área de sistemas.	30 días
32	Supervisar el cumplimiento del reglamento de crédito actualizado.	30 días
33	Supervisar el cumplimiento del reglamento de sistemas.	30 días
34	Supervisar que los requisitos legales y regulatorios se cubran y cumplan de forma eficiente.	30 días

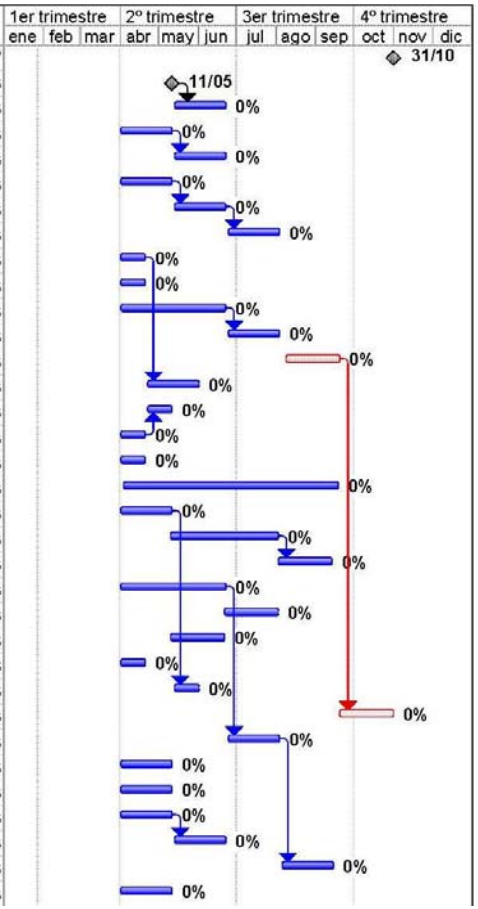


Figura 4.1. Cronograma de Actividades del Plan de Acción

La Tabla 4.8 muestra el plan de acción de las actividades con los responsables y costos aproximados de implementación.

Tabla 4.8. Plan de Acción.

ACTIVIDAD	RESPONSABLE
Definir políticas de seguridad, confidencialidad y procesos internos.	Consultor externo
Revisión, aprobación y difusión de las políticas de seguridad, confidencialidad y procesos internos.	Consejo de Administración Gerente General
Definición de un plan de acción documentado y formal para evaluación de riesgos crediticios.	Consultor externo
Revisión, aprobación y difusión del plan de acción para evaluación de riesgos crediticios.	Consejo de Administración Gerente General
Definición de un plan de acción documentado y formal para evaluación de riesgos de TI.	Consultor externo
Revisión, aprobación y difusión del plan de acción para evaluación de riesgos de TI.	Gerente General Jefe de Sistemas
Implementar la gestión de riegos de TI.	Jefe de Sistemas Operador de sistemas y soporte al usuario
Actualizar el sistema operativo de los servidores a Microsoft Windows Server 2008 R2 Standard w/SP1.	Jefe de Sistemas Operador de sistemas y soporte al usuario
Actualizar el sistema operativo de las terminales de la cooperativa por el MS OEM Windows 7 Profesional SP1.	Jefe de Sistemas Operador de sistemas y soporte al usuario
Elaboración de un plan de contingencias, que permita evaluar y minimizar interrupciones de los servicios prestados propios del sistema, análisis de puntos de falla y administración de problemas, también se debe incluir seguridad en la estructura física del departamento de sistemas y de la red.	Consultor externo
Revisión, aprobación y difusión del plan de contingencias	Gerente General Jefe de Sistemas
Implementar el plan de contingencias	Jefe de Sistemas Operador de sistemas y soporte al usuario
Resolver los problemas de seguridad de la red, derechos de acceso, riesgo de errores, fraudes, alteración no autorizada o accidental.	Consultor externo
Adquirir un antivirus para los dos servidores, recomendable Enterprise Security for Endpoints - Server Protect de la marca Trend Micro.	Jefe de Sistemas Operador de sistemas y soporte al usuario

Adquirir un antivirus para las catorce terminales por Enterprise Security for Endpoints- Ofiice Scan de la marca Trend Micro.	Jefe de Sistemas Operador de sistemas y soporte al usuario
Adquirir mecanismos de seguridad para restringir a personal no autorizado el acceso a la información física de los socios de crédito.	Gerente General
Adquirir un nuevo software financiero de acuerdo a los requerimientos de la cooperativa y capacitar al personal en su manejo.	Proveedor externo
Actualizar y difundir el reglamento de crédito.	Consejo de Vigilancia Gerente General
Formular un manual de procedimientos de gestión interna para el departamento de crédito.	Consultor externo
Revisión, aprobación y difusión del manual de procedimientos de gestión interna para el departamento de crédito.	Consejo de Administración Gerente General
Elaborar un reglamento para el departamento de sistemas.	Consultor externo
Revisión, aprobación y difusión del reglamento para el departamento de sistemas.	Consejo de Administración Gerente General Jefe de Sistemas
Implementar un proceso de seguimiento y control de las acciones de cobranza de la cartera de crédito.	Consejo de Administración Gerente General
Automatizar la elaboración del informe de crédito y del pagaré de crédito.	Jefe de Sistemas Operador de sistemas y soporte al usuario
Capacitar al personal, para de esta manera evitar posibles errores o riesgos que puedan producirse en los procesos o aplicaciones.	Consultor externo
Incorporar eventos de simulacro dentro del entrenamiento de la contingencia para una respuesta a la verificación efectiva del personal en situaciones de crisis.	Consultor externo
Concienciar y capacitar a todo el personal de la cooperativa acerca de la importancia de la seguridad tanto a nivel de software como de hardware.	Consultor externo
Estructurar un inventario de los recursos críticos de software y hardware de la cooperativa.	Jefe de Sistemas Operador de sistemas y soporte al usuario
Definir, documentar y difundir un programa de monitoreo y control interno para el área de crédito.	Auditor externo
Definir, documentar y difundir un programa de monitoreo y control interno para el área de sistemas.	Auditor informático
Supervisar el cumplimiento del reglamento de crédito actualizado.	Auditor interno
Supervisar el cumplimiento del reglamento de sistemas.	Auditor informático

Supervisar que los requisitos legales y regulatorios se cubran y cumplan de forma eficiente.	Auditor externo

APROXIMACIÓN DE COSTOS

De acuerdo con la investigación realizada, en la Tabla 4.9 se presentan los costos estimados para los diferentes componentes considerados en el plan de acción, como recursos humanos, adquisición de equipos y de software, materiales y suministros e imprevistos. Las cifras se presentan en dólares estadounidenses.

Para efectos de la estimación se han considerado los siguientes supuestos:

- Para el jefe de sistemas, operador de sistemas y soporte al usuario, auditor interno, gerente general, Consejo de Administración, Consejo de Vigilancia, se estima el mismo salario que reciben mensualmente.
- Para el puesto del auditor informático se ha considerado la misma categoría del profesional informático actual.
- Las estimaciones de costos de software se fundamentan en cotizaciones obtenidas por algunos distribuidores nacionales.
- Se considera la adquisición una estación de trabajo, que corresponde al faltante para el auditor informático, con procesador Core I7, velocidad de 2.8Ghz, 4Gb de memoria RAM, 1000Gb de disco duro.
- El costo del equipo se estimó según datos proporcionados por distribuidores de equipos.

Tabla 4.9. Presupuesto del plan de acción.

PRESUPUESTO DEL PLAN DE ACCIÓN DE DE LA COOPERATIVA DE AHORRO Y CREDITO "FORTUNA" PERÍODO MAYO-OCTUBRE 2012				
RECURSOS HUMANOS	**N.-**	**COSTO/ MES**	**MESES**	**VALOR**
Consultor externo de seguridades	1	3600.00	2	7200.00
Consultor externo de control interno	1	3600.00	2	7200.00
Consultor externo de riesgos	1	3600.00	2	7200.00
Auditor informático	1	1000.00	2	2000.00
Auditor interno	1	1000.00	2	2000.00
Jefe de sistemas	1	1000.00	2	2000.00
Consejo de vigilancia	3	250.00	2	1500.00
Consejo de administración	5	250.00	2	2500.00
Gerente general	1	1500.00	2	3000.00
Operador de sistemas y soporte al usuario	1	500.00	2	1000.00
Capacitación	1	3000.00	2	6000.00
HERRAMIENTAS TECNOLÓGICAS				
Licencia de Microsoft Windows Server 2008 R2 Standard w/SP1.	2	1003.52		2007.04
Licencia de MS OEM Windows 7 Profesional SP1.	14	208.32		2916.48

Licencia de Enterprise Security for Endpoints - Server Protect de la marca Trend Micro	2	50.40		100.80
Licencia de Enterprise Security for Endpoints- Ofiice Scan de la marca Trend Micro	14	50.40		705.60
Software financiero	1	85000.00		85000.00
Adquisición de equipo	1	900.00		900.00
MATERIALES Y SUMINISTROS				3000.00
IMPREVISTOS				3000.00
TOTAL				**$139,229.92**

El tiempo estimado para llevar a cabo el plan de acción es de aproximadamente siete meses, y con un costo total de $139229.92

Con el planteamiento de las actividades del plan de acción, se pretende facilitar la toma de decisiones por parte de los directivos de la cooperativa, las cuales asociadas con la introducción y consolidación de la auditoría informática establecen una cultura de la seguridad y una excelencia en el tratamiento de la información en todos sus procesos de negocio, permitiéndole a ésta llegar a un nivel de madurez superior al actual. Así, aporta a la cooperativa un valor añadido de reconocido prestigio, en la calidad de los servicios que ofrece a sus socios.

Un aspecto fundamental para que se lleve a cabo este plan de acción es el compromiso de la administración de la institución, la cual debe asumir la responsabilidad que le es propia en cuanto al diseño, actualización e implantación del sistema de control interno. Por grandes que sean los esfuerzos y aportes de la auditoría, no habrá valor agregado en tanto la administración no asuma este papel y se comprometa con la implantación de las recomendaciones propuestas.

Otro aspecto a considerar para la ejecución del plan de acción es la disponibilidad de recursos, la administración debe asignar los recursos financieros y humanos requeridos para la implantación de la propuesta.

Cabe mencionar que la propuesta de mejora de, implementación de servidores virtualizados, planteada en el apartado anterior se podría llevar a cabo a largo plazo, conforme se vaya resolviendo lo urgente que es lo detallado en el plan de acción.

El no implementar del plan de acción propuesto, dejara a la cooperativa estancada y no alcanzará la mejora contínua para servir eficientemente a los socios, así como contrarrestar el riesgo operativo, que es lo que la organización tiene propuesto en uno de sus objetivos.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Una vez finalizado el trabajo de investigación se tienen como conclusiones las siguientes:

- Se conocieron los procedimientos crediticios internos de la cooperativa, pudiéndose determinar que los procesos de crédito son realizados en un 40% mediante un sistema automatizado y el 60% de estos procesos de crédito son realizados de forma manual, lo que supone un coste alto, tanto en recursos como en tiempo de trabajo para las oficiales de crédito de la institución.

- El sistema con el que trabaja la cooperativa no garantiza confianza en cuanto a la veracidad y consistencia de la información, ya que se deben realizar muchos procesos de forma manual, lo cual retrasa la ejecución de las actividades en los diferentes departamentos, pudiendo generarse errores, por lo tanto este aplicativo no se adapta a las necesidades de la cooperativa.

- La consecución de un nivel de madurez mayor al actual en base a los objetivos de control del marco referencial COBIT, se logrará a través de la aplicación del plan de acción planteado en la presente tesis.

- Si bien existe un plan de acción a seguir, hay que tener en cuenta que debe haber un enfoque de mejora contínua, es decir; un proceso evolutivo, cuya consolidación demandará esfuerzo y tiempo, siendo el avance de la tecnología de la información uno de los factores que marcará la pauta para lograrlo.

- Existe una gran cantidad de herramientas computarizadas de apoyo a la función de auditoría, su adecuada utilización puede redundar en significativos beneficios para las organizaciones, siendo de especial relevancia una adecuada selección conforme a los requerimientos y características institucionales.

RECOMENDACIONES

Una vez realizada la ejecución de la auditoría informática se recomienda lo siguiente:

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

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

- En base a los lineamientos que define el marco de trabajo COBIT, junto con la adopción de mejores prácticas de TI y la implementación del plan de acción recomendado, tanto para el departamento de crédito como en el departamento de sistemas de la cooperativa, ésta podrá elevar su nivel de madurez actual y así mejorar su competitividad.

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

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

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

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

GLOSARIO

AUDITOR
Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular. [54]

AUDITORÍA
Es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas. [1]

Conjunto de métodos y técnicas con los que se procura identificar y evaluar algo.

AUDITORÍA INFORMÁTICA
Es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos. [1]

AUDITOR INFORMÁTICO
Evalúa y comprueba en determinados momentos del tiempo los controles y procedimientos informáticos más complejos, desarrollando y aplicando técnicas mecanizadas de auditoría, incluyendo el uso del software [1].

AUDITORÍA DE PROCESOS
Es una rama de la auditoría interna. Contar con un proceso estandarizado y documentado sobre la forma como debe realizarse la supervisión de actividades de una función las cuales arrojen resultados para la mejora continua con el fin de determinar el cumplimiento de los indicadores establecidos dentro de una organización.[46]

BASE DE DATOS
Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. [51]

BURÓ DE CRÉDITO
Reporte al que se accede vía internet y debe ser contratado por la entidad financiera, en el cual por medio del número de cedula se puede consultar el historial crediticio de una persona.

COBIT
Marco de referencia de buenas prácticas para el control de TI. Acrónimo en inglés de Objetivos de Control para la Información y la Tecnología Relacionada, emitido por el IT Governance Institute®. [2]

COMITÉ DE CRÉDITO
Gerente y socios fundadores de la cooperativa elegidos para la revisión de las solicitudes de crédito.

CONTROL
"Las Políticas, Procedimientos, Prácticas y Estructura Organizacional, diseñadas para proveer una razonable seguridad de que los objetivos del negocio serán alcanzados y los eventos indeseados serán prevenidos o detectados y corregidos."[50]

CONTROL INTERNO
"Cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos. [14]

CONEXUS
Sistema financiero utilizado en la Cooperativa de Ahorro y Crédito "Fortuna"

CRÉDITO
Uso de los fondos de alguien más a cambio de una promesa de pago (generalmente con intereses) en una fecha posterior. [59]

DOMINIO
Agrupación de objetivos de control en etapas lógicas en el ciclo de vida de inversión en TI. [2]

ESTÁNDAR
Modelo que se sigue para realizar un proceso. Producto de *software* o *hardware* que cumple determinadas reglas fijadas por acuerdo internacional, nacional o industrial. [53]

EVALUACIÓN DE RIESGOS
Evaluar de forma recurrente la posibilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La posibilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio. [53]

GESTIÓN DE RIESGOS
Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. [54]

GOBIERNO DE TI
"Es responsabilidad del consejo de administración y de la dirección ejecutiva. Es una parte integral del gobierno corporativo y consiste en el liderazgo y estructuras de organización y procesos que aseguran que la tecnología de información de la empresa ofrece sustento a los objetivos y estrategias de la organización". [47]

GOVERNANCE INSTITUTE
El (ITGI, por sus siglas en Inglés) (*www.itgi.org*) se estableció en 1998 para evolucionar el pensamiento y los estándares internacionales respecto a la dirección y control de la tecnología de información de una empresa. Un gobierno de TI efectivo, ayuda a garantizar que la TI soporte las metas del negocio, optimice la inversión del negocio en TI, y administre de forma adecuada los riesgos y oportunidades asociados a la TI. El IT Governance Institute ofrece

investigación original, recursos electrónicos y casos de estudio para ayudar a los líderes de las empresas y a sus consejos directivos en sus responsabilidades de Gobierno de TI. [2]

HALLAZGO:
Debilidades, deficiencias o brechas apreciables respecto a un criterio o estándar previamente definido. [58]

INTEGRIDAD DE LA INFORMACIÓN
Se refiere al valor del contenido de la información con el tiempo y generalmente se relaciona al trabajo del autor o creador. [2]

INFORMACIÓN
Conjunto organizado de datos procesados, que constituyen un mensaje sobre un determinado ente o fenómeno.

ISACA *Information Systems Audit and Control Association* (www.isaca.org)
Systems Audit and Control Association Information (Asociación de Auditores de Procesamiento Electrónico de Datos). Publica COBIT y emite diversas acreditaciones en el ámbito de la seguridad de la información. [54]

LISTA DE CHEQUEO
Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. [54]

MARCO DE TRABAJO (framework)
Un conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular que sirve como referencia para enfrentar y resolver nuevos problemas de índole similar. [48]

MEDIO DE APROBACIÓN
Documento en Excel en donde se resume toda la información que el socio llenó en la solicitud de crédito.

MODELO DE MADUREZ
Método de puntaje de modo que una organización pueda calificarse a sí misma desde inexistente hasta optimizada (de 0 a 5). [58]

n/a
No hay respuesta, no aplicable, no disponible

NIVEL DE MADUREZ
Modelo utilizado por muchas organizaciones para identificar las mejores prácticas, las cuales son convenientes para ayudarles a evaluar y mejorarla madurez de su proceso de desarrollo de software. [2]

OBJETIVO DE CONTROL
Una declaración del resultado o propósito que se desea alcanzar al Implementar procedimientos de control en un proceso en particular. [58]

PAGARÉ
Documento legal que respalda una operación de crédito.

POLÍTICA
Por lo general, un documento que ofrece un principio de alto nivel o una estrategia a seguir. El propósito de una política es influenciar y guiar la toma de decisiones presente y futura, haciendo que estén de acuerdo a la filosofía, objetivos y planes estratégicos establecidos por los equipos gerenciales de la empresa. Además del contenido de la política, esta debe describir las consecuencias de la falta de cumplimiento de la misma, el mecanismo para manejo de excepciones y la manera en que se verificará y medirá el cumplimiento de la política. [2]

PLAN ESTRATÉGICO DE TI
Conjunto de definiciones tecnológicas e iniciativas de TI que deben soportar la visión, misión y estrategias que el negocio tiene para un horizonte de tiempo definido.

PROCESO
Por lo general, un conjunto de procedimientos influenciados por las políticas y estándares de la organización, que toma las entradas provenientes de un número de fuentes, incluyendo otros procesos, manipula las entradas, y genera salidas, incluyendo a otros procesos, para los clientes de los procesos. Los procesos tienen razones claras de negocio para existir, dueños responsables, roles claro y responsabilidades alrededor de la ejecución del proceso, así como los medios para medir el desempeño. [2]

PROCEDIMIENTO
Es un método de ejecutar una serie común de pasos definidos que permite realizar un trabajo en forma correcta.

QUINQUENAL
Repetitivo cada cinco años. [1]

RED
Sistema de comunicación entre computadoras que permite la transmisión de datos de una máquina a otra.

RIESGO
Es la vulnerabilidad de los bienes de una institución ante un posible o potencial perjuicio o daño.

RPC
Del inglés Remote Procedure Call (Llamada a Procedimiento Remoto), es un protocolo que permite a un programa de ordenador ejecutar código en otra máquina remota sin tener que preocuparse por las comunicaciones entre ambos. [61]

SERVIDOR VIRTUALIZADO
Servidor virtual dedicado o privado (VPS), una partición dentro de un servidor físico que habilita varias máquinas virtuales dentro de dicha máquina por medio del uso de diversas tecnologías. [63]

SISTEMA INFORMÁTICO
Un sistema informático es un conjunto de partes que funcionan relacionándose entre sí con un objetivo preciso.

SISTEMA DE ADMINISTRACIÓN DE LIBRERÍAS DE MEDIOS
Un inventario físico de los medios magnéticos almacenados. [2]

SID (identificador único para la sesión de usuario)
Identificador de seguridad, es un número utilizado para identificar a usuarios, grupos y cuentas de equipo en Windows. [62]

SOFTWARE ENGINEERING INSTITUTE (SEI SEI: http://www.sei.cmu.edu/)

Es un instituto federal estadounidense de investigación y desarrollo, fundado por el Congreso de los Estados Unidos en 1984 para desarrollar modelos de evaluación y mejora en el desarrollo de software, que dieran respuesta a los problemas que generaba al ejército estadounidense la programación e integración de los sub-sistemas de software en la construcción de complejos sistemas militares. Financiado por el Departamento de Defensa de los Estados Unidos y administrado por la Universidad Carnegie Mellón. [58]

TABLA DE AMORTIZACIÓN
Detalle de los pagos con número de cuota, fecha de pago, valor capital, valor de interés, valor de seguro de desgravamen, otros (mora, judicial), total de la cuota y saldo capital.

TI
Tecnología de Información, conjunto de técnicas que permiten la captura, almacenamiento, transformación, transmisión y presentación de la información generada o recibida a partir de procesos, de manera que pueda ser organizada y utilizada en forma consistente y comprensible por los usuarios que estén relacionados con ella. Incluye elementos de hardware, software, telecomunicaciones y conectividad. [58]

TIRILLA
Detalle numérico del valor a acreditar realizado en la maquina sumadora.

BIBLIOGRAFÍA

[1] Piattini M. y Del Peso E. (2007). *Auditoría Informática, un enfoque práctico*. México 2007, 2da. Edición

[2] It Governance Institute. *Cobit 4.1.* (2007), Estados Unidos, [En Línea]. Disponible en: www.itgi.org, http://www.isaca.org/Knowledge-Center/cobit/Documents/cobiT4.1spanish.pdf [Consulta 18-01-2011]

[3] Lardent A. y Hall P. (2001). *Sistemas de Información Para Gestión Empresarial: Procedimientos, Seguridad y Auditoría*.

[4] Echenique J. y McGraw H. (2001). *Auditoría en Informática*.

[5 Santo Domingo A. (1997). *Introducción a la informática*. Editorial Ariel S.A.

[6] García S. (1997). *"Auditoría Informática I: Nota técnica para el curso"*. Costa Rica.

[7] Hevia Vázquez E. (1999). *Concepto Moderno de la Auditoría Interna*. España.

[8] It Governance Institute. (2000). *Directrices de Auditoría COBIT vs 3.0*.

[9] Velastegui Sánchez T. (2008). *Tesis Análisis de la Gestión de las Tecnologías de la Información en la Unidad de Gestión de la Información de la EPN usando COBIT.* Ecuador.

[10] Caiza A. y Matute M. (2007). *Tesis Evaluación de Riesgos en empresas desarrolladoras de Software utilizando la herramienta MSAT*. Ecuador.

[11] Calderón Yong F. A. (2010), *Tesis AUDITORÍA INFORMÁTICA APLICANDO COBIT 4.0 EN LA COOPERATIVA DE AHORRO Y CRÉDITO "PABLO MUÑOZ VEGA" LTD*A, Ecuador – Tulcán.

[12] *Soluciones en Ingeniería de Gestión,* (2009), [En Línea], Disponible en: http://es.scribd.com/doc/40028764/normas-calidad [Consulta 21-02-2011]

[13] Fonseca Borja R. (2004). *Auditoría Interna, Un enfoque moderno de planificación, Ejecución y control*. Guatemala.

[14] Sobrinos R. (1999). La Mancha. (2011). [En Línea] Disponible en: http://alarcos.inf-cr.uclm.es/per/fruiz/cur/mso/comple/Cobit.pdf[Consulta 01-18-2011]

[15] Ricardo Vilches. (2008). *Apuntes del estudiante de auditoría,* [En Línea], Disponible en: http://www.gestiopolis.com/recursos4/docs/fin/apuestaud.htm [Consulta 18-01-2011]

[16] Lugmaña F. y Recalde L. (2009). *Procedimiento para realizar auditoría de procesos ti sobre plataformas Windows utilizando herramientas comerciales*, [En Línea]. Disponible en: http://bibdigital.epn.edu.ec/bitstream/15000/1133/1/CD-1978.pdf [Consulta 18-01-2011]

[17]Documento disponible en: http://www.mioruro.com/libros/derecho/Todas%20Leyes%20Bolivianas/CLASES_DE_AUDITOR_A_GUBERNA.DOC [Consulta 11-02-2011]

[18] *Auditoría Informática de los sistemas de información de la ESPE Dominio de Planeación y Organización*. [En Línea]. Disponible en: http://www3.espe.edu.ec:8700/bitstream/21000/723/1/T-ESPE-021849.pdf [Consulta 23-10-2011]

[19] Landacay K. (2010). *Tesis Definición de un marco de gobierno de TI para la UTPL*. Ecuador.

[20] Gonzales Narváez G. (2008), *Auditoría Informática A Una Institución Del Sector Financiero Agencia* Guayaquil. [En Línea] http://www.dspace.espol.edu.ec/handle/123456789/4884/1/7660.pdf [Consulta 28-03-2011]

[21] Álvarez F. (2007), *El control interno basado en COBIT*. [Consulta 27-05-2010]

[22]Cooperativa Fortuna, Disponible en: http://cooperativafortuna.com/index.php?option=com_content&task=view&id=5&Itemid=39 [Consulta 02-02-2011]

[23] *Tipos de auditorías y conceptos básicos*. [En Línea]. Disponible en: http://es.scribd.com/doc/22224605/2-Tipos-de-Auditoría [Consulta 11-02-2011]

[24] Guzmán de León C. (2000), *Lineamientos Generales para una Auditoría de Sistemas en el centro de Información de una Institución Bancaria*. [En Línea]. Guatemala. Disponible en: http://issuu.com/oiram96/docs/12916/#download [Consulta 28-03-2011]

[25] COBIT, DIRECTRICES DE AUDITORÍA, Julio de 2000, 3a Edición, Emitido por el Comité Directivo de COBIT y El IT Governance Institute TM

[26] Vandama N.; Lescay M.; Castillo G. y García F. *Auditoría Informática en ETECSA*. [En Línea]. Cuba. Disponible en: http://espejos.unesco.org.uy/simplac2002/Ponencias/Segurm%E1tica/VIR024.doc [Consulta 25-03-2011]

[27] Einnova, *Estándares TI*. [En Línea]. Disponible en: http://auditoríasistemas.com/estandares-ti/ [Consulta 08-04-2011]

[28]ISO 27000: *Sistemas de seguridad de la información*. [En Línea]. Disponible en: http://www.iso27000.es/iso27000.html [Consulta 09-04-2011]

[29] *Normas para la seguridad del software*. (2007). [En Línea]. Documento Disponible en: icicm.com/files/NormasCalSegSoftware.doc [Consulta 09-04-2011]

[30]*ISO/IEC 15404: SPICE.* [En Línea]. Disponible en: http://ingenieria.ucaldas.edu.co/auditoría/index.php/ISO/IEC_15404:SPICE,_ISO/IEC_15408:2005,_ISO/IEC_19770:2006_ISO_12207 [Consulta 09-04-2011]

[31]*IT Baseline Protection Manual.* [En Línea]. Disponible en: http://ingenieria.ucaldas.edu.co/auditoría/index.php/IT_Baseline_Protection_Manual_(BPM) [Consulta 02-07-2011]

[32] CaseWare. [En Línea]. Disponible en: http://www.caseware.com/products/idea [Consulta 15-08-2011]

[33]*Datasec, Meycor Cobit Guías de auditoría. [En Línea].* Disponible en*:* http://www.datasec-soft.com/sp/content/view/9/12/ [Consulta 09-04-2011]

[34] Computer *Assisted Audit Techniques CAAT: Capítulo 3. Legislación informática, mejores prácticas y técnicas de auditoría informática.* [En Línea]. Disponible en. http://olea.org/~yuri/propuesta-implantacion-auditoría-informática-organo-legislativo/ch03s04.html [Consulta 11-04-2011]

[35] Auditoría de sistemas. [En Línea]. Disponible en: http://naizona.blogspot.com/2009/08/v-behaviorurldefaultvml-o.html [Consulta 04-02-2011]

[36] Wikipedia, TickIT. [En Línea]. Disponible en: http://es.wikipedia.org/wiki/TickIT [Consulta 09-04-2011]

[37]Wikipedia, Modelo de Capacidad y Madurez. [En Línea]. Disponible en: http://es.wikipedia.org/wiki/Modelo_de_Capacidad_y_Madurez [Consulta 12-04-2011]

[38] Brito Domínguez J. (2009). Tesis: *Creación de un Marco de Control para la Administración del Riesgo Operativo relacionado con la Tecnología de Información como modelo para las Cooperativas de Ahorro y Crédito del Ecuador*. [En Línea]. Ecuador. Disponible en: http://www.docstoc.com/docs/48942061/Creacin-de-un-Marco-de-Control-para-la-Administracin [Consulta 13-05-2011]

[39] Balseca S. y Cachimuel M. (2008). *Evaluación y auditoría informática del sistema de información de la escuela politécnica del ejército: dominio entrega de servicios y soporte* [En Línea]. Ecuador. Disponible en: http://www3.espe.edu.ec:8700/bitstream/21000/688/1/T-ESPE-021854.pdf [Consulta 25-10-2011]

[40] Peralta A.; Núñez J.; Hernández V y Hilario F. (2011). *Auditoría de Aplicaciones y Base de Datos.* [En Línea]. Disponible en: http://www.slideshare.net/Fausto_Hilario/infouditor-srl-analisis-foda [Consulta 05-11-2011]

[41] IT GOVERNANCE INSTITUTE, ISACA (2006): COBIT 4.0.

[42]Comparación de Controles Internos: COBIT, SAC y COSO. [En Línea]. Disponible en: http://www.netconsul.com/riesgos/cci.pdf [Consulta 01-18-2011]

[43] Sarmiento R. *El Proceso General de Auditoría, Instituto Sonorense de Contadores Públicos.*

[44] *Manual de procedimientos de Auditoría Interna*, Universidad de Buenos Aires.

[45] Mg. Flores A, SISBIB, *Auditoría a los procesos en las empresas*, (2003).

[46] Instituto Mexicano de contadores públicos, *Auditoría de procesos.*

[47] *Gobierno de TI.* [En Línea]. Disponible en: http://es.scribd.com/doc/52944054/Auditoría-Informática-00-Gobierno-de-TI [Consulta 10-02-2011]

[48] Wikipedia, *Framework*. [En Línea]. Disponible en http://es.wikipedia.org/wiki/Framework [Consulta 03-03-2011]

[49]ISACA, [En Línea]. Página oficial: http://www.isaca.org/About-ISACA/History/Espanol/Pages/default.aspx [Consulta 10-02-2011]

[50]Pallavicine C. *COBIT*, [En Línea]. Disponible en: www.dspace.espol.edu.ec/bitstream/123456789/5300/2/COBIT.ppt [Consulta 28-09-2011]

[51]Definición disponible: http://www.pergaminovirtual.com.ar/definicion/Base_de_datos.html [Consulta 08-27-2011]

[52] Definición disponible: http://es.thefreedictionary.com/est%C3%A1ndar [Consulta 08-27-2011]

[53] COBIT 4.0. (2006). *Control Objetives Management Guidelines Maturity Models*. [En Línea]. E.E.U.U. Disponible en: www.securitycn.net/img/uploadimg/20070831/cobit4.0_en.pdf [Consulta 18-01-2011]

[54] Definición disponible en: http://arm-net.com.ar/es/glosario.html [Consulta 08-27-2011]

[55] Endara Néjer F. *Estudio de la Metodología COBIT: IT Governance y Control Objetives, aplicados a la Auditoría y Seguridad Informática.*

[56] Coronel Hoyos K. (2008). Tesis: *Metodología de evaluación del riesgo tecnológico en las instituciones del sistema financiero ecuatoriano, utilizando COBIT* 4.1 [En Línea]. Ecuador. Disponible en: www3.espe.edu.ec:8700/bitstream/21000/410/1/T-ESPE-021885.pdf [Consulta 09-29-2011]

[57] Lara H.; Reyes J. y Navarrete W. (2006). *Diseño de Sistema de Gestión de Seguridad de Información para Ecuacolor* [En Línea]. Ecuador. Disponible en: http://www.dspace.espol.edu.ec/handle/123456789/6962/7/Tesis [Consulta 09-21-2011]

[58] Superintendencia General de entidades Financieras (2008), *Guía para completar la Matriz de Calificación de la Gestión de TI*, [En Línea]. Costa Rica. Disponible en: http://www.sugef.fi.cr/servicios/documentos/normativa/Reglamento%2014-

09/Descarga/FormulariosyGuias/Guía%20para%20completar%20la%20Matriz%20de%20Calificación.pdf [Consulta 18-01-2011]

[59] Samuelson P. (2006). *Economía*. México 2006, 18ava. Edición

[60] *RPC*, Disponible en: http://www.slideshare.net/crack_708/rpc

[61] I*dentificador de Seguridad* [En línea]. Disponible en: http://pays-talmondais.com/od/termss/g/security-identifier.htm?-Identificador-de-seguridad-Definici%C3%B3n-(SID) [Consulta 05-10-2011]

[62] UNDERMEDIA S.A**.** (2002 – 2011). *Servidores dedicados virtuales* [En línea]. Ecuador. Disponible en: http://www.mangohosting.com/servidores/servidores-dedicados-virtuales/ [Consulta 05-11-2011]

[63] *Nessus 4.4 User Guide* [En Línea]. Disponible en: http://static.tenable.com/documentation/nessus_4.4_user_guide.pdf [Consulta 12-08-2011]

LISTA ANEXOS

Los anexos están disponibles en el CD de esta memoria en la carpeta Anexos. Cuyos documentos tienen distintos formatos, entre ellos: PDF, DOC, XLS, JPG, TXT y HTML; cuyo nombre está disponible en orden secuencial.

ANEXO	DESCRIPCIÓN
Anexo 1	**Documento técnicas de auditoría** Descripción de las principales técnicas de auditoría, que incluye partes básicas del plan de trabajo de un auditor informático y el proceso que se debe realizar en una auditoría informática.
Anexo 2	**Documento objetivos de control** Definición de los objetivos y procesos de control del marco referencial COBIT, además se define los controles generales de TI y controles de aplicación.
Anexo 3	**Módulos del sistema "CONEXUS"** Presenta un listado de los módulos existentes en el sistema con el que trabaja la cooperativa.
Anexo 4	**Formato medio de aprobación** Formato realizado en Excel que sirve como medio de aprobación del crédito solicitado por el socio a la cooperativa "Fortuna".
Anexo 5	**Formato pagaré y formato contrato de préstamo** Formato de pagaré del contrato de préstamo de la cooperativa "Fortuna", especificando el monto del crédito solicitado y los datos de los firmantes del crédito.
Anexo 6	**Formato notificaciones** Formato de notificación al socio en caso de no cumplir con los plazos de pago establecidos.
Anexo 7	**Cuestionario para evaluar el control interno a gerencia** Documento que incluye el cuestionario realizado a gerencia para evaluar el control interno en la cooperativa.
Anexo 8	**Cuestionario para evaluar el control interno en el departamento de crédito** Documento con preguntas que se ha realizado a las oficiales de crédito para evaluar el control interno.

Anexo 9	**Cuestionario para evaluar el control interno mediante COBIT al área informática** Cuestionario realizado al jefe de sistemas para evaluar el control interno en el área de informática.
Anexo 10	**Formato de créditos demandados** Incluye datos de los socios con créditos vencidos más de noventa días y que están en trámite de demanda judicial.
Anexo 11	**Reglamento de crédito** Documento que incluye el Reglamento de crédito de la cooperativa "Fortuna".
Anexo 12	**Acta de resolución del Consejo de Administración** Documento de constatación de la existencia de las actas de resolución del Consejo de Administración.
Anexo 13	**Acta comité de crédito** Documento de constatación de la existencia de las actas del comité de crédito.
Anexo 14	**Acta manual del sistema informatico de la cooperativa** Documento de constatación de la existencia del manual de usuario del sistema con el que trabaja la cooperativa.
Anexo 15	**Acta inventario CD´S** Documento de constatación de la existencia de respaldos en CD´s de la base de datos de la cooperativa.
Anexo 16	**Dominios, procesos y objetivos de control de COBIT** Definición de todos los dominios, procesos y objetivos de control del marco referencial COBIT.
Anexo 17	**Informe final de auditoría** Documento del Informe final de la auditoría.
Anexo 18	**Acta informe de auditoría** Documento de constatación de informes de auditorías realizadas al departamento de crédito.
Anexo 19	**Acta reglamento interno de trabajo** Documento de constatación de la existencia del reglamento interno de trabajo de la cooperativa
Anexo 20	**Acta código de conducta de ética** Documento de constatación de la existencia del código de conducta y ética de la cooperativa.

Anexo 21	**Manual de crédito/cartera** Documento que incluye un manual de procedimientos de crédito y cartera.
Anexo 22	**Matriz de evaluación** Documento en excel que incluye la matriz de evaluación y la definición de los procesos seleccionados con sus respectivos objetivos de control que se utilizó para realizar la auditoría en la cooperativa, en base a los modelos de madurez.
Anexo 23	**Reporte NESSUS** Resultados de la ejecución de la herramienta NESSUS que se ejecutó para la detección de vulnerabilidades en el servidor de Base de Datos, servidor DNS y equipos utilizados en el área de crédito.
Anexo 24	**Buró de crédito** Reporte al que se accede vía internet y debe ser contratado por la entidad financiera, en el cual por medio del número de cedula se puede consultar el historial crediticio de una persona.
Anexo 25	**Solicitud de crédito deudor** Formato de solicitud de crédito que realiza el socio a la cooperativa.
Anexo 26	**Certificado de depósito de ahorro** Formato de certificado de depósito de ahorro a plazo de la cooperativa.
Anexo 27	**Nombramiento gerente** Nombramiento del gerente general de la cooperativa "Fortuna".
Anexo 28	**Tabla de amortización** Formato de una tabla de amortización de la cooperativa "Fortuna", que contiene información del cliente y los créditos solicitados.
Anexo 29	**Reportes TotalCréditosConcedidos** Documento en Excel que contiene datos de créditos concedidos obtenidos de la base de datos de la cooperativa.
Anexo 30	**Estado económico del cliente** Información del estado económico del cliente, tomado del sistema "CONEXUS".
Anexo 31	**Estado económico del garante** Formato de estado de situación personal de la persona que servirá como garante del crédito.
Anexo 32	**Propuesta** Descripción e información de la propuesta operativa para los servidores virtualizados.

Anexo 33	**Reporte Créditos Vencidos** Documento en Excel que contiene datos de créditos vencidos, obtenidos de la base de datos de la cooperativa.
Anexo 34	**Reporte Cálculo de mora** Documento en Excel que contiene datos de créditos vencidos y sus respectivas moras, obtenidos de la base de datos de la cooperativa.
Anexo 35	**Reportes Créditos vencidos1** Documento en Excel que contiene datos de créditos vencidos que permiten comparar bases de datos.
Anexo 36	**Reportes Créditos vencidos y demandados** Documento en Excel que contiene datos de créditos vencidos y que están demandados en la cooperativa.
Anexo 37	**Reportes Créditos Concedidos** Documento en Excel que contiene datos de todos los créditos concedidos sean estos vigentes o cancelados desde Enero del 2004 hasta Septiembre del 2011, obtenidos de la base de datos de la cooperativa.

ANEXOS

PAPER