ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN
Y TRANSFERENCIA DE TECNOLOGÍA
UNIDAD DE GESTIÓN DE POSTGRADOS

TESIS DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE:
MAGISTER EN EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS
II PROMOCIÓN

TEMA: "AUDITORÍA BASADA EN COSO ERM A LA GESTIÓN DE RIESGO OPERATIVO PARA LA COAC ALIANZA DEL VALLE"

AUTOR: OBANDO, CÉSAR ANTONIO

DIRECTOR: ING. BERMEO, PAULO
CODIRECTOR: ECO. CHIRIBOGA, GABRIEL

SANGOLQUÍ, MARZO DEL 2014

CERTIFICACIÓN

Certificamos que el presente trabajo titulado: AUDITORÍA BASADA EN COSO ERM A LA GESTIÓN DE RIESGO OPERATIVO PARA LA COAC ALIANZA DEL VALLE, fue realizado en su totalidad por el ingeniero César Antonio Obando Changuán, bajo nuestra supervisión, y cumple con las normas estatutarias establecidas por la ESPE en el Reglamento de Estudiantes de la Universidad de las Fuerzas Armadas.

Sangolquí, Enero del 2014

……	……
Ing. Paulo Bermeo M., MBA	Eco. Gabriel Chiriboga, MSi.
DIRECTOR	OPONENTE

AUTORÍA DE RESPONSABILIDAD

La Tesis de Grado Titulada : AUDITORÍA BASADA EN COSO ERM A LA GESTIÓN DE RIESGO OPERATIVO PARA LA COAC ALIANZA DEL VALLE, ha sido desarrollada en base a una investigación, respetando derechos intelectuales de terceros, cuyas fuentes son citadas e incorporadas en la bibliografía, en cuanto a los datos financieros y operativos utilizados para la auditoría son supuestos, esto respetando el derecho a la confidencialidad de la información que protege a la institución.

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

Sangolquí, Enero del 2014

……

Ing. César Antonio Obando Ch.

CI: 0400866414

AUTORIZACIÓN

Yo, César Antonio Obando Changuán, autorizo a la Universidad de las Fuerzas Armadas, ESPE, la publicación en la biblioteca virtual de la institución del trabajo de la tesis “AUDITORÍA BASADA EN COSO ERM A LA GESTIÓN DE RIESGO OPERATIVO PARA LA COAC ALIANZA DEL VALLE”, cuyo contenido es de mi responsabilidad.

Sangolquí, enero 2014

…….

Ing. César Antonio Obando

CI: 0400866414

DEDICATORIA

Dedico este trabajo principalmente a Dios, por haberme dado la vida y permitirme llegar hasta este momento tan importante de mi formación profesional. A mi esposa Bremilda, por ser pilar fundamental y demostrarme siempre su amor y apoyo incondicional sin importar nuestras diferencias de opiniones y a pesar de nuestra distancia física, siento que estás conmigo siempre. A mis hijos Jean Karlo, Daniel, Jhosué, a quienes quiero mucho, por compartir momentos significativos conmigo y por siempre estar dispuestos a escucharme y ayudarme.

AGRADECIMIENTO

Este proyecto es el resultado del esfuerzo conjunto de todos. Por esto agradezco a mi director de tesis, Ing. Paulo Bermeo y oponente Eco. Gabriel Chiriboga. A mis profesores a quienes les debo gran parte de mis conocimientos, gracias a su paciencia y enseñanza y finalmente un eterno agradecimiento a esta prestigiosa universidad la cual abrió y abre sus puertas a personas como nosotros, preparándonos para un futuro competitivo y formándonos como personas de bien.

INDICE

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

RESUMEN

La tesis está enfocada a un examen de Auditoría a la Gestión de Riesgo Operativo basado en COSO ERM para COAC Alianza del Valle, que posee un marco referencial no estandarizado para gestionar y administrar los riesgos operativos, se establecen los siguientes objetivos específicos: identificar las ventajas y desventajas de utilizar COSO ERM como marco de referencia y su viabilidad en la auditoria de la cooperativa, definir y analizar la relación entre los procesos, personas, tecnología y eventos externos en los cuales se centra el riesgo operativo como factor que la eficiencia y productividad de la COAC Alianza del Valle, identificar los principales riesgos operativos a los que puede estar expuesta la cooperativa y cómo el marco de referencia COSO ERM puede ayudar para identificarlos y mejorar la eficiencia y productividad de la COAC Alianza del Valle, se desarrolla mapas y matrices de riesgos que ayuden a tener una perspectiva integral de la gestión del riesgo operativo identificando naturaleza, causas, probabilidades e impacto, se utiliza un plan de auditoría contemplando principalmente los riesgos tecnológicos según la Resolución No JB-2005-834, los hallazgos y las recomendaciones encontrados apuntan a la necesidad de formalización, finalizando en un dictamen sobre el nivel de madurez que tiene la administración.

Palabras clave

COSO, RIESGO, CONTROL, EVIDENCIA, HALLAZGO

CAPÍTULO I

Auditoría basada en Coso ERM a la Gestión de Riesgo Operativo para la COAC Alianza del Valle

Los cambios que se han dado como consecuencia de la crisis financiera del 2008; originada en el sector financiero y bancario en los EE.UU de Norteamérica, que entraron en eventos de crisis por varios factores de riesgos entre ellos la falta de supervisión de las instituciones reguladas, han ayudado a que se implementen instrumentos especializados para el monitoreo, control y mitigación de los riesgos en las gestiones del sistemas financiero.

Las instituciones financieras se han visto obligadas a especializar el recurso humano para mantener credibilidad en el mercado. Se han implementado instrumentos en la administración de los riesgos financieros, tales como: crédito, mercado y riesgo operativo. En el caso del riesgo operativo está implícito las perdidas por las fallas tecnológicas, errores de liquidez transaccional, inundaciones, fuego, robo terrorismo, fallas humanas, de procesos, además los eventos externos de la cooperativa, por lo tanto la auditoria informática identifica como se está gestionando los riesgos corporativos que deben ser cuantificados, monitoreados para mitigar las perdidas por el riesgo operativo.

En este contexto, el propósito de este trabajo es realizar una auditoría informática con marco de referencia COSO ERM a la gestión del riesgo operativo según la resolución de la Junta Bancaria N. JB-2005-834 de 20 de

octubre del 2005, en el capítulo V De la Gestión del Riesgo Operativo a Cooperativa de Ahorro Crédito Alianza del Valle con énfasis en riesgo tecnológico, recalcando en que la información que se utiliza es ficticia, esto debido al derecho a la confidencialidad de la información que protege a la cooperativa.

A través de este trabajo lo que se pretende es demostrar las ventajas y bondades de realizar una auditoría enmarcada en COSO ERM, para lo cual se elabora inicialmente un plan de auditoria que cubre los siguientes aspectos: revisión de preliminares, revisión detallada, evaluación de la información, pruebas de cumplimiento y sustanciación, aplicación de controles y comunicación de resultados, para finalizar se redacta el informe final de auditoría evidenciando los hallazgos para cada uno de los componentes COSO ERM y su respectivas recomendaciones.

1.1 Justificación e importancia

Según la (Agenda Política Económica del Buen Vivir, 2011) la nueva visión de la economía para el Buen Vivir tiene, que se deriva de la aplicación de la Constitución Política del 2008 plantea objetivos claros como:

a) Mejorar la calidad y esperanza de vida y aumentar las capacidades y potencialidades de la población.

b) Construir un sistema económico, justo, democrático, productivo, solidario y sostenible, basado en la distribución igualitaria de los beneficios del

desarrollo, de los medios de producción y en la generación de trabajo digno y estable.

c) Garantizar la soberanía nacional, promover la integración latinoamericana e impulsar nuestra inserción estratégica e inteligente en el mundo.

La Cooperativa está enmarcada en el sector de la Economía Popular y Solidaria y cuyo objetivo es "impulsar las iniciativas de organización cooperativa, asociativa y comunitaria sinérgica de los propios recursos y capacidades de los actores de la EPS, para resolver sus necesidades mediante la producción social y ecológicamente responsable de bienes y servicios necesarios para la convivencia social, comercializados a precios justos y generando excedentes económicos que sean reinvertidos en la sociedad y en su localidad" (MIES, 2010-2013) por lo tanto, esta tesis basada en los objetivos descritos anteriormente pretende contribuir a través de la auditoria a la Gestión de Riesgos de la Cooperativa Alianza del Valle en la construcción de una economía equitativa, instaurando procesos, procedimientos y medidas de control interno instalados en la entidad e integrados dentro de sus procedimientos operativos y administrativos, con miras a promover la formación de socios y clientes, conocedores de sus derechos y protagonistas de su "buen vivir".

Es bueno recalcar que toda entidad financiera que aplique controles sobre los riesgos en todas sus operaciones conducirá a tener un sistema más ágil, que permita tener una planificación que sea capaz de verificar que esos controles se cumplan para darle una mejor visión a la gestión, bajo estándares

internacionales que garanticen un nivel de madurez adecuado y una mejora continua en función de la cadena de valor del negocio.

Administrar y gestionar riesgos forma parte del negocio cotidiano y necesario de los bancos o entidades afines para poder lograr beneficios y generar valor para sus partes interesadas , esto principalmente debido a que la mayor parte del fondeo de una institución financiera se basa en los ahorros de los depositantes, siendo por tanto indispensable una mayor rigurosidad en el control y seguimiento de las entidades financieras (Riesgo Moral, Gobierno Corporativo), para ello el Comité de Basilea presentó en 1997 veinticinco principios para una supervisión bancaria efectiva; en 1999 implementó su metodología debido a novedades importantes en materia de regulación y supervisión en dónde; en el 2004, especialmente para el enfoque de la administración de riesgos, actualizó sus principios e incorporó el principio séptimo “Proceso de Administración de Riesgos” y otros pilares fundamentales como fueron los de requerimiento mínimo de capital y disciplina de mercado.

En 1997 se solicitan cambios para las entidades financieras dentro de la Comisión de Basilea I y en el 2004 por Basilea II sobre gobierno corporativo, controles y riesgos, haciéndolos efectivo como obligatorios por la Superintendencia Bancos y Seguros, con resolución No. JB-2005-834 del 20 de octubre del 2005, incorporando la norma como Capítulo V “De la gestión del riesgo operativo” del título X “De la Gestión y Administración de Riesgos” para las entidades vigiladas, y ahora por la Superintendencia de la Economía Popular y Solidaria.

1.2 Planteamiento del problema

La Cooperativa de Ahorro y Crédito “Alianza del Valle Ltda.” de la ciudad de Quito provincia de Pichincha hasta diciembre del 2012 estaba bajo la supervisión y control de la Superintendencia de Bancos y Seguros, cumpliendo con las normativas y regulaciones de la Gestión de Riesgos y Administración de Riesgos emitidos según resolución de la Junta Bancaria N. JB-2005-834 de 20 de octubre del 2005, en el capítulo V De la Gestión del Riesgo Operativo.

A partir del 27 de febrero de 2012 según decreto N. 1061 del Registro Oficial Suplemento 648 se instituye “Que la Constitución de la República en su artículo 283 establece que el sistema económico se integrará por las formas de organización económica pública, privada, mixta, popular y solidaria, y las demás que la Constitución determine; y, que la economía popular y solidaría se regulará de acuerdo con la ley e incluirá a los sectores cooperativistas, asociativos y comunitarios;..” (Registro Oficial No. 1061, 2012)

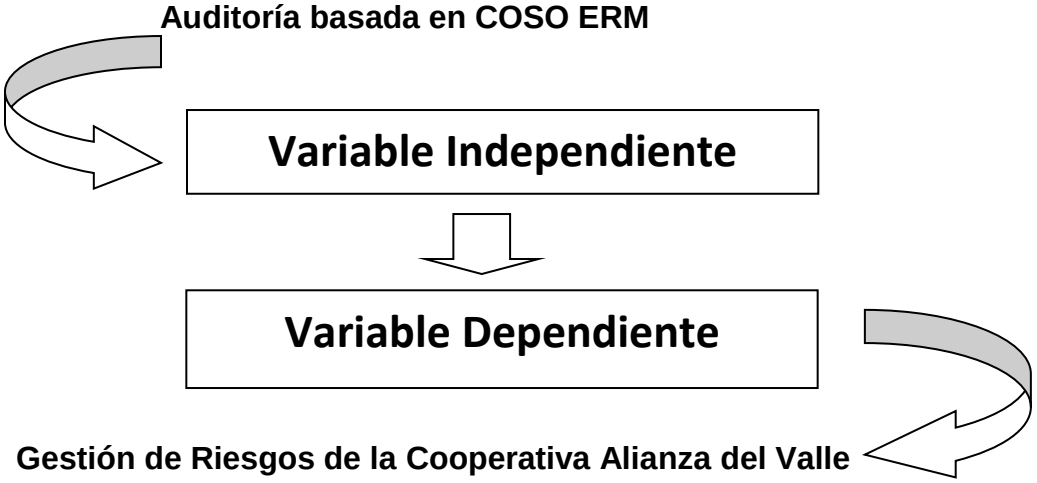
Dentro de la estructura organizacional de la Cooperativa se tiene un Comité de Riesgos encargado de la gestión de los eventos de riesgos bajo normativas externas (Superintendencia de Bancos y Seguros), y en la actualidad por la nueva Superintendencia de Economía Popular y Solidaria complementada por la normatividad interna, que coadyuvan a la gestión financiera.

La COAC Alianza del Valle no posee un marco referencial para la gestión de los riesgos operativos y la administración de los riesgos por lo que es necesario tener identificados y organizados los riesgos que accionan la cadena

de valor del negocio y de esta forma mitigarlos antes de que se materialicen, especialmente nos centraremos en el riesgo tecnológico considerando que si bien es cierto el software , en el Ecuador tiene un nivel adecuado para aplicar a las distintas herramientas diseñadas para medir el riesgo operativo el inconveniente radica en la velocidad que se dan los cambios y encontrar las herramientas adecuadas.

1.3 Formulación del problema

El propósito de esta tesis es auditar a la Cooperativa Alianza del Valle y más específicamente las áreas relacionados con riesgos operativos utilizando el marco de referencia COSO ERM, para determinar los principales riesgos operativos a los que puede estar expuesto la COAC Alianza del Valle si no aplica controles internos adecuados, evaluarlos y mitigarlos de tal forma que impidan las pérdidas financieras cuidando la reputación y evitando eventos potenciales que impidan la continuidad de sus operaciones así como de las ventajas y desventajas de utilizar un marco de referencia para gestionar los riesgos operativos de la COAC Alianza del Valle.



1.4 Objetivo general

Realizar la Auditoría basada en COSO ERM a la Gestión de Riesgo Operativo para COAC Alianza del Valle.

1.5 Objetivos específicos

- ✓ Identificar las ventajas y desventajas de utilizar COSO ERM como marco de referencia y su viabilidad en la auditoría de la COAC Alianza del Valle.
- ✓ Definir y analizar la relación entre los procesos, personas, tecnología y eventos externos en los cuales se centra el riesgo operativo como factor que la eficiencia y productividad de la COAC Alianza del Valle.
- ✓ Identificar los principales riesgos operativos a los que puede estar expuesta la COAC Alianza del Valle y cómo el marco de referencia COSO ERM puede ayudar para identificarlos y mejorar la eficiencia y productividad de la COAC Alianza del Valle.
- ✓ Desarrollar mapas y matrices de riesgos que ayuden a tener una perspectiva integral de la gestión del riesgo operativo identificando naturaleza causas, probabilidades e impacto.
- ✓ Determinar los riesgos que requieren un tratamiento prioritario y sugerir los mecanismos para tratarlo.

CAPÍTULO II

2.1 Marco teórico

2.1.1 Antecedentes del estado del arte

Las Cooperativas de Ahorro y Crédito en el Ecuador han asumido un rol protagónico en la trasformación financiera con una buena aceptación en la población, quienes manifiestan haber encontrado en las Cooperativas de Ahorro y Crédito la oportunidad de acceder a productos y servicios financieros de forma oportuna y eficaz. La transformación se ha dado en el ámbito operacional y financiero trayendo como consecuencia un crecimiento en cobertura, productos y servicios parecidos a los de la Banca, tomando como plataforma de apoyo estratégico la tecnología y sus ramas afines.

Esa trasformación traducida en crecimiento y el uso de la tecnología ha contribuido para que las COAC's tengan un grado de madurez muy alto de dependencia y coyunturalmente que los riesgos que están relacionados con las tecnologías de información se trasfieran a los diferentes procesos del giro del negocio.

Organizaciones internacionales al igual que las gubernamentales del Ecuador, han emitido una serie de regulaciones, normativas, normas y mejores prácticas como: COBIT, ISO 27001, COSO ERM y la Resolución de la Junta Bancaria 834 y ejecutada hacia las instituciones financieras controladas por la Superintendencia de Bancos del Ecuador, que permite a las Cooperativas en particular implementar una buena administración y gestión del Riesgo Operativo

(Procesos, Tecnología, Eventos Externos, Personas) dictada por Basilea II que se basa en tres pilares y uno de ellos es los Riesgos. La evolución tanto de los mercados financieros de Ecuador y la globalización muy presente hoy en día, como la regulación que está presente es más especializada en lograr una medición de riesgos más completa objetiva y cuantitativa.

En el acuerdo de Basilea II en su contexto hace un enfoque a los capitales que serán aplicados al sector Bancario, haciendo historia de cómo se ha ido posicionando los acuerdos podemos mencionar.

Tabla 1: Acuerdos Basilea II

Año	Actividad Relevante
1998	Acuerdo Original de Basilea I
1994	Efecto Tequila (Crisis Financiera)
1996	Primera enmienda de Riesgo de Mercado
1997	Crisis Asiática (Rusa, Turquia), Brasil, Fractura de necesidad de cambio
1999	Principios básicos de La supervisión bancaria
1999	Acuerdos nuevos de Basilea II

El nuevo acuerdo está basado en:

Tabla 2: Nuevos acuerdos Basilea II

Año	Actividad Relevante
1999	Se da los nuevos acuerdos de Basilea II
2000	Principios para la Administración de Riesgos de crédito
2001	Segunda consultiva, para la administración y supervisión de riesgo Operativo
2003	Tercera consultiva
2004	Acuerdo definitivo
2006 hasta 2010	Implementación y Regulaciones bancarias

En la actualidad los riesgos operacionales, y de manera particular el fraude, pueden hacer desaparecer a entidades financieras de mayor o menor

importancia, además en algunos casos ha llegado a poner en riesgo al sistema financiero completo de un país, de una región e incluso de todo el mundo. En la tabla se expone algunas entidades bancarias que tuvieron un remezón por causas del riesgo operativo.

Tabla 3: Ejemplos de colapsos bancarios

INSTITUCIÓN	CAUSA
Barings Bank fundado en 1762 en Inglaterra, logró renombre por múltiples operaciones históricas, adquisición de Luisiana por los EE.UU.	Banco fue declarado en quiebra, cerrando las operaciones, riesgo operacional de la violación a las normas de doble supervisión y ocultamiento de operaciones perdidas.
Jerome Kerviel operador de bolsa más famoso del mundo, en el 2008 hizo que el banco francés Societé Générale perdiera alrededor de cinco mil millones de euro en una serie de operaciones bursátiles	Acusado de falsificación y uso de documentos falsos, por abuso de confianza y de ingresar datos informáticos al sistema del banco.
La Familia Peirano, padre, y tres hijos relacionados a los bancos Mercantiles (Uruguay), Alemán (Paraguay), Velox(Argentina) y Trade and Commerce Bank (Cayman).	Este caso fue lleno de incidentes procesales, extradición, prisión, libertad provisional, anulación del proceso en Uruguay y por haberse derogado la ley.
Crisis financiera del año 2003, En principios se pensaba que los bancos afectados eran víctimas de ciertos factores externos, ajenos a ellos, que afectaban su situación de liquidez, pero que no existían problemas de solvencia.	La crisis financiera del 2003, originada en fraudes bancarios, llevó al Banco Mundial y al Banco Interamericano de Desarrollo a publicar un comunicado conjunto en el que expresaban lo siguiente: "En el caso de Baninter, la crisis económica provocó un deterioro significativo del ingreso real y aumentó en un 50 por ciento el número de pobres en el país, registrando así un millón y medio de pobres, de los cuales 670,000 alcanzaron la pobreza extrema."

Fuente:http://www.santiagodigital.net/index.php?option=com_content&task=view&id=1169

El riesgo operacional y de manera particular el fraude bancario, tienen la capacidad de desencadenar una crisis que traspase rápidamente las fronteras de la entidad o del país donde se inicia, por lo que debe ser objeto de atención.

En el Ecuador un elemento que ha causado incidentes de riesgo operativo en el sector financiero es el no tener el suficiente conocimiento sobre el Lavado de Activos para tratar este riesgo, lo que conlleva afirmar que éste riesgo, sumado la seguridad de la información, y el control de riesgos tecnológicos, son asuntos que han preocupado a las instituciones en general y en especial a las financieras en los últimos años. El conocimiento sobre cómo tratar estos riesgos es fundamental en materia (Lavado de Activos) y fraudes o delitos informáticos a largo plazo y saber que se deben afinar los procesos de prevención y control.

En términos de Riesgo Operativo, frente a otros países, nuestro país, está en una etapa inicial, ya que la normativa emitida por la Superintendencia tiene fechas de cumplimiento recientes, a diferencia de otros países donde dicha normativa data del 2006, por lo que ha sido mejorada e interiorizada por las organizaciones.

Existen varios tratados sobre auditorías y evaluación de Riesgos en las instituciones financieras y en especial de las Cooperativas de Ahorro y Crédito del país (Brito, 2009) en su tesis elaborada en la Escuela Politécnica del Litoral, hace una exposición amplia de la administración de riesgo operativo relacionado a la tecnología de la información orientado a las Cooperativas de Ahorro y Crédito.

(Ferreas Salegre, 2005) de la Unidad Central de Riesgos Operativos del BBVA el 13 de octubre de 2005 realiza una exposición de ciertas consideraciones relativas al uso avanzado de modelos de medición, donde expone los modelos de medición del riesgo operativo en España luego de la publicación en mayo de 2004 y que entra en vigencia en la Banca desde 2007 – 2008 donde se incluye una provisión de capital por riesgo operacional y considerando que cuando la gestión del riesgo sea mínima el nivel de gestión del riesgo será por un conocimiento bajo del conocimiento de la entidad.

El Magister Manuel Espinoza Cruz, realiza un tratado denominado “La Auditoria y sus Paradigmas”, donde plantea tres hipótesis orientadas a buscar evidencia de la gestión de una auditoria en el siglo XIX, auditorías del desempeño basadas en los riesgos del sistema operativo y por ultimo hace referencia que las auditorías son individuales a la naturaleza de cada institución.

En el evento realizado por la Superintendencia de Bancos en enero de 2005, en la exposición realizada por la Intendencia de Supervisión de Riesgos, cuya temática es el Riesgo Operacional Bases Conceptuales, se expone que el riego operativo no es una práctica nueva, las organizaciones siempre han buscado prevenir, reducir, los errores en procesos transaccionales, como se había analizado el riesgo operativo tuvo un tratamiento cualitativo en las auditorías internas, no se le daba la importancia como para darle un marco de referencia importante.

En este taller la Superintendencia de Bancos y Seguros del Ecuador expone que se ha incrementado el riesgo de operación por las siguientes causas: Incremento del comercio electrónico, sistemas informáticos sin control, Productos complejos, Servicios tercerizados en aumento, Oferta y demanda de servicios.

Tabla 4: Delitos Informáticos

INSTITUCIÓN	DELITOS INFORMÁTICOS EN ECUADOR
GMS y Kaspersky Lab presentaron el estudio "Delitos Cibernéticos en el Ecuador"	El estudio demuestra que entre el 2009 y 2010 el Ecuador tuvo un incremento del 360% de crimen cibernético. Dmitry Bestuzhev, Senior Regional Researcher de América Latina de Kaspersky Lab, indica que "el 94% de todos los programas de código malicioso hospedados en los servidores Web del Ecuador se encuentran en la provincia del Pichincha. Además está previsto para el presente año el delito informático incrementará en un porcentaje incluso mayor al 100%. El Ecuador cuenta con el 61% de ataques cibernéticos son en Pichincha y las provincias que reflejan menor grado de violaciones de seguridad informática son Guayas y Azuay con el 20% y 7% respectivamente.
EL DELITO INFORMÁTICO EN EL ECUADOR "UNA NUEVA TENDENCIA CRIMINAL DEL SIGLO XXI" SU EVOLUCIÓN, PUNIBILIDAD Y PROCESO PENAL [Alexander Cuenca Espinosa]	En el año 2009 en el Ecuador ya se puso en discusión el tema de imponer penas a los delitos informáticos. Estas penas que se impondrían fueron ya discutidas en el proyecto para la creación de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, ley que un principio tuvo sus falencia por el desconocimiento de la materia, es decir, por el desconocimiento por parte de profesionales en cuanto a delitos informáticos, ya que como es obvio era una tendencia criminal que iniciaba en el país.
MUNICICIPIO DEL DISTRITO METROPOLITANO DE QUITO	Ataque a la página del Municipio de Quito en el año 2001. Vale recordar también que el primer delito informático que se cometió en el Ecuador fue en el año 1996, en un caso conocido, que fue denunciado pero que nunca obtuvo sentencia: el redondeo de cantidades que se efectuaba en las planillas realizadas por el antiguo EMETEL, caso en el cual se desconocía a donde se dirigían estas cantidades (que muchas veces eran demasiado pequeñas para que cause discusión), pero que juntadas, formaban un monto de dinero muy apreciable. Para este tipo de delito informático se utilizó la técnica del Salami o Rounding Down.
BURÓ DE ANÁLISIS INFORMATIVO	Los delitos informáticos han crecido sobretodo en los últimos dos años. En el 2009 se registraron 168 casos; en el 2010, 1.337; y entre enero y junio de 2011, 1.366; según las denuncias registradas en la Fiscalía

	General del Estado, que engloba las cifras de todo el país. Esto significa que en el primer semestre de este año, ya hay 23 casos más de los denunciados durante todo el año pasado. Estos fraudes a través de internet podrían significar un perjuicio de por lo menos un millón de dólares, según informes de la Dirección Nacional de Tecnologías de la Información de la Fiscalía. En marzo de este año, había más de 1.600 causas rezagadas desde enero de 2010. De ahí que tanto la Superintendencia de Bancos y la Fiscalía firmaron una resolución mediante la cual las entidades financieras se comprometieron a restituir el 100% del dinero sustraído por medio de robos electrónicos.
LA HORA (Los delitos informáticos no paran) (lunes, 14 de noviembre de 2011)	En los últimos tres años ha existido un crecimiento alarmante de los delitos informáticos. En 2009 se denunciaron en la Fiscalía 168 casos de fraude informático y en 2010 se llegó a 1.099. En lo que va del 2011 la cifra asciende a 1.366 denuncias. La Fiscalía y la SBS decidieron, a principios del 2011, coordinar acciones y conformar una comisión para investigar estos hechos. Según cálculos oficiales, habría 1.500 personas perjudicadas por un monto de cerca de 3 millones de dólares. La Fiscalía da cuenta que la Superintendencia deberá ordenar a los bancos la restitución total de los montos que han sido defraudados a sus clientes. En ese documento se insiste en la necesidad de que la entidad de control deberá estudiar la posibilidad de contratar una póliza de fidelidad bancaria, que incluyan específicamente a la cobertura denominada delito informático y cibercriminal, que brinde amparo contra fraudes bajo condiciones entre clientes y Banco.
ECUADOR TENDENCIAS EMPRESARIALES [http://www.ecuadortrends.com/index.php?option=com_content&view=article&id=308:se-presento-el-estudio-delitos-ciberneticos-en-el-ecuador-en-la-puce&catid=31:eventos&Itemid=27], [martes 26 de abril de 2011]	La Asociación de las Escuelas de Comunicación y Derecho de la Pontifica Universidad Católica del Ecuador PUCE con el apoyo de GMS y Kaspersky presentaron la conferencia Delitos informáticos en el Ecuador ¿Por qué los criminales te quieren tanto?, dictada por el especialista en seguridad informática Dmitry Bestuzhev, Senior Regional Researcher de América Latina de Kaspersky Lab. Dmitry Bestuzhev, Senior Regional Researcher de América Latina de Kaspersky Lab, indica que “el 94% de todos los programas de código malicioso hospedados en los servidores Web del Ecuador se encuentran en la Pichincha. Además está previsto para el presente año el delito informático incrementará en un porcentaje incluso mayor al 100%. El Ecuador cuenta con el 61% de ataques cibernéticos son en Pichincha y las provincias que reflejan menor grado de violaciones de seguridad informática son Guayas y Azuay con el 20% y 7% respectivamente.

2.1.2 Marco Teórico

Originariamente, la auditoría se limitó a las verificaciones de los registros contables, dedicándose a observar si los mismos eran exactos, confrontando lo escrito con las pruebas de lo acontecido y las respectivas referencias de los registros.

Con el tiempo, la auditoría ha continuado creciendo, el informe SAC (Sistema de Auditoría y Control) define a un sistema de control interno como: "un conjunto de procesos, funciones, actividades, subsistemas, y gente que son agrupados o conscientemente segregados para asegurar el logro efectivo de los objetivos y metas"**.**

El control interno está diseñado e implementado por la administración para tratar los riesgos de negocio y de fraude identificados que amenazan el logro de los objetivos establecidos, tales como la confiabilidad de la información financiera.

El control interno es un medio para alcanzar un fin y no un fin en sí mismo, lo llevan a cabo las personas que conducen en todos los niveles, no se trata solamente de manuales de organización y procedimientos, sólo puede aportar un grado de seguridad razonable y no la seguridad total para la conducción o consecución de los objetivos.

El "Informe COSO", publicado en Estados Unidos en 1992, nació como respuesta a las inquietudes sobre una variedad de conceptos, definiciones e interpretaciones que existían respecto al control interno. (COSO ERM, 2004)

El objetivo primordial del Informe COSO ERM es ayudar a las organizaciones a mejorar el control de sus actividades, estableciendo un marco para los conceptos del control interno que permita una definición común del control interno y la identificación de sus componentes.

Hacia fines de Septiembre de 2004, el Committee of Sponsoring Organizations of the Treadway Commission, publicó el Enterprise Risk Management y sus aplicaciones técnicas asociadas, ampliando el concepto de control interno, proporcionando un foco más robusto y extenso sobre la identificación, evaluación y gestión integral de riesgo, donde se incorpora el marco de control interno permitiendo a las compañías mejorar sus prácticas de control interno o decidir encaminarse hacia un proceso más completo de gestión de riesgo. (Sistema Bibliotecario Matias, 2004).

A medida que acelera el ritmo de cambio, la mayoría de las organizaciones necesitarán mejorar su capacidad de aprovechar oportunidades, evitar riesgos y manejar la incertidumbre. Esta nueva metodología proporciona la estructura conceptual y el camino para lograrlo. La premisa principal de la gestión integral de riesgo es que cada entidad, con o sin fines de lucro, existe para proveer valor a sus distintos “grupos de interés”. (López, 2005).

2.1.3 Marco conceptual

Riesgo: “Se lo puede definir como la volatilidad o dispersión de los resultados esperados, en base a los movimientos de las variables financieras y operacionales”. (Brito, 2009)

Riesgo Operativo: Según Basilea II, el riesgo operativo se define como riesgo de pérdida debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos o bien a causa de los acontecimientos externos. (Báez, 2010).

Clasificación del Riesgo: Los riesgos que puede enfrentar una institución financiera son: [Clasificación del Riesgo Financiero Basado en Modelos De Calificación Difusos].

Riesgo Operativo.- Es la probabilidad que ocurra pérdidas financieras, originadas por incidentes o debilidades de procesos, personas, sistemas internos, tecnología, y conjugado con eventos externos imprevistos, no se considera las pérdidas ocasionadas por cambios en el entorno político, económico y social. (Universidad de la República de Uruguay, Control Interno, 2012)

Riesgo Tecnológico.- El riesgo tecnológico tiene su origen en el continuo incremento de herramientas y aplicaciones tecnológicas que no cuentan con una gestión adecuada de seguridad. Su incursión en las organizaciones se debe a que la tecnología está siendo fin y medio de ataques debido a vulnerabilidades existentes por medidas de protección inapropiadas y por su constante cambio, factores que hacen cada vez más difícil mantener actualizadas esas medidas de seguridad. (Revista Seguridad, 2009)

Sistema Financiero.- Se puede definir al sistema financiero como un conjunto de instituciones, instrumentos y mercados donde se va a canalizar el ahorro hacia la inversión, en el cual juegan un papel muy importante los intermediarios financieros cuya función principal será canalizar el ahorro hacia

la inversión, tomando en cuentas las necesidades de los ahorristas. (García, 2010)

Control Interno.- SAC (Sistema de Auditoría y Control) define a un sistema de control interno como: “un conjunto de procesos, funciones, actividades, subsistemas, y gente que son agrupados o conscientemente segregados para asegurar el logro efectivo de los objetivos y metas. (Net Consul.com, 2012)

Ambiente de Control.- componente que se relaciona con la cultura organizacional de la entidad, estableciendo la alta dirección normas de conducta adecuadas bajo principios éticos y honestos que sean adoptados por los miembros de la organización y sus actividades sean desarrolladas bajos ciertos principios. (Universidad de la República de Uruguay, Control Interno, 2012)

Evaluación de Riesgos.- Concientización de las entidades financieras que existen riesgos internos y externos a los cuales están expuestos, debiendo identificar y evaluar cuáles podrían ser las causas y sus potenciales eventos, comparándolos con los objetivos de la organización. (Alfaro, 2008)

Actividades de Control.- Delimita las políticas y procedimientos de control para minimizar la ocurrencia y el posible impacto de los riesgos identificados. (Brito, 2009)

Información y comunicación.- La Alta dirección garantiza que existe una adecuada comunicación de las directrices políticas y procedimientos a nivel de toda la organización de tal manera que sea conocida por los miembros, la

información debe estar disponible para correcta operación de sus actividades. (Brito, 2009)

Monitoreo.- Seguimiento de la aplicación de las políticas de control interno en cada una de las áreas de la organización, de tal forma, que se pueda encontrar confiabilidad y oportunidad de las deficiencias existentes para tomar acciones correctivas e inmediatas. (Dirección y Coordinación Técnica de Planificación, 2011)

COSO ERM o COSO II.- Committee of Sponsoring Organizations of the Treadway Commission, enuncio um marco de control mejorado del COSO, denominado COSO –ERM, (Enterprise Risk Management), basado en el riesgo. (Net Consul.com, 2012)

Establecimiento de Objetivos.- La alta dirección define los objetivos de la organización y defina los potenciales eventos que pudieran ser evitados bajo ciertos parámetros formales de análisis. (Coso, 2004)

Identificación de Eventos.- La Alta Dirección debe realizar un análisis de cuáles son los eventos o acontecimientos internos y externos que afectan a la organización, tanto a nivel interno y externo, de tal forma, que se los puede catalogar como oportunidades o riesgos. (Monografias.com)

Evaluación de Riesgos.- Establece que los riesgos deben ser analizados en forma detallada determinado cuales son las causas que pudieran provocarlo y el nivel de impacto para la organización. (COSO ERM, 2004)

Respuesta al Riesgo.- Determina qué va hacer con riesgos a los cuales está expuesta la organización, que puede evitar, aceptar, reducir o compartir los riesgos. (Net Consul.com, 2012)

Actividad de Control.- Se determina las políticas, procesos, y procedimientos encaminados a tomar las acciones de respuesta al riesgo que anteriormente fueron analizados y establecidos. (Brito, 2009)

Supervisión.- Establecer los mecanismos apropiados para determinar si los componentes anteriores se están cumpliendo cabalmente para que se puedan tomar las acciones correspondientes y necesarias. (Brito, 2009)

CAPÍTULO III

3.1 Metodología

Las organizaciones que necesitan mejorar su capacidad de aprovechar oportunidades, evitar riesgos y manejar la incertidumbre, requieren implementar metodología de administración de riesgos y una buena evaluación y auditoria.

La metodología proporciona la estructura conceptual y el camino a seguir, a través de la Auditoria basado en COSO ERM a los riesgos operativos de la Cooperativa Alianza del Valle queremos lograr que la institución consiga ubicarse en esta estructura con la premisa principal que la gestión integral de riesgo, que cada entidad, independiente a su naturaleza, provee valor a sus distintos “grupos de interés”.

Sin embargo, todas estas entidades enfrentan incertidumbres y el desafío para la administración es determinar el apetito al riesgo que la entidad está dispuesta aceptar, y buscar el incrementar el valor de esos “grupos de interés”.

La incertidumbre es generada por factores externos a la entidad como eventos externos, tecnología, reestructuraciones, cambios en los mercados, competencia y regulaciones, y por factores internos como las elecciones estratégicas de la organización. La incertidumbre emana de la inhabilidad para determinar con precisión la probabilidad asociada a la ocurrencia de un evento y a sus impactos correspondientes. El valor es creado, preservado o desgastado por las decisiones de la administración en todas las actividades,

desde la planificación estratégica a la operación del día a día. Es por esto que COSO ERM describe un marco basado en principios que provee lo siguiente:

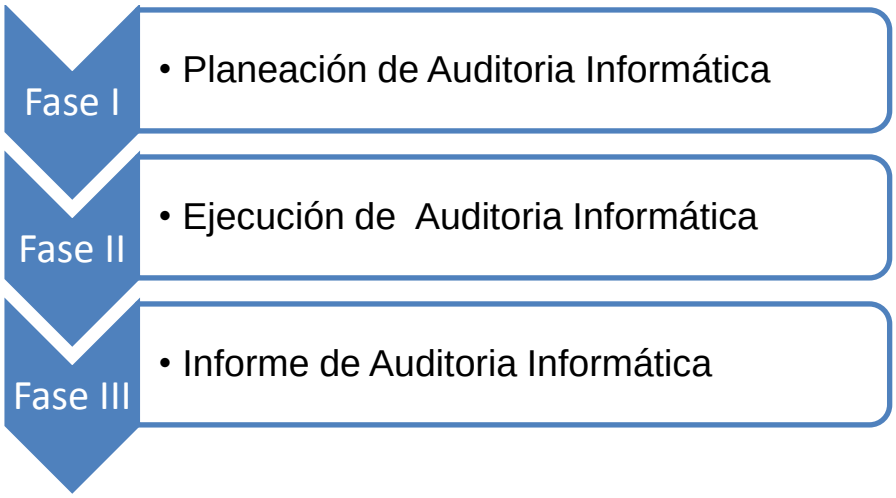
- La definición de administración de riesgos corporativos.
- Los principios críticos y componentes de un proceso de administración de riesgos corporativos efectivo.
- Pautas para las organizaciones sobre cómo mejorar su administración de riesgos.
- Criterios para determinar si la administración de riesgos es efectiva, y si no lo es que se necesita para que lo sea.

COSO ERM está conformado por 8 componentes que se relacionan entre sí, estos son:

- Ambiente de Control
- Establecimiento de Objetivos.
- Identificación de eventos.
- Evaluación de Riesgos.
- Respuesta al Riesgo.
- Actividades de Control.
- Información y Comunicación.
- Monitoreo.

En la metodología se plantea seguir las siguientes fases:

Gráfico 1: Etapas de auditoría



3.1.1 Fase I: Planeación de la auditoría informática

La auditoría informática como técnica y herramienta de apoyo en las instituciones, han facilitado en las últimos años el desarrollo en las áreas de Sistemas. La información se adquiere importancia primordial y se convierte en un activo intangible, irrecuperable e invaluable.

En la planeación de la auditoria que realizamos en este trabajo, se revisa y evalúa los controles, sistemas y procedimientos de informática, de los equipos de cómputo, su utilización, eficiencia y seguridad, para sugerir cursos alternativos para una utilización más eficiente y segura de la información, donde se considera cada uno de los elementos de COSO ERM, utilizando varias estrategias como lectura de documentos, encuestas, entrevistas.

PLAN DE AUDITORÍA			
No.	**Actividad**	**Estrategia**	**Medio de verificación**
REVISIÓN DE PRELIMINARES			
a	Cobertura de la Auditoría		
	Objetivos de la Auditoría		
	Alcance de la auditoría		
b	Comprensión del Negocio a ser auditado	Lectura de documentos	Ficha técnica
	Ubicación Geográfica y Económica		
	Procesos de Negocio		
	Procesos gobernantes		
	Procesos operativos		
	Procesos de soporte		
REVISIÓN DETALLADA			
a	Comprensión de los proceso de negocio	Planificación estratégica	Documento
	Modelo de Negocio		
	Estructura Orgánica		
	Objetivos de la Organización		
	Estratégicos, Operativos		
b	Reportes confiables		
c	Cumplimiento (Normas internas y Externas)		
d	Planeación y documentos relacionados		
e	Declaración del Código de Ética		
f	Declaración de Visión, Misión, Valores		
g	Productos y Servicios		
h	Gobierno Cooperativo		
i	Control interno		
j	Entorno de TI en un Contexto de Negocio		
EVALUACIÓN DE LA INFORMACIÓN			
a	Área a ser Auditada	Técnica de Auditoría	Procesos
	Operativo		
	Tecnológico (SBS-834)		
b	Identificación de Objetivos y Riesgos		
	Riesgo Aceptado		
	Tolerancia al Riesgo		

	Matriz de objetivos y Riesgos Críticos		
	Riesgos Operativos		
	Tecnológico (SBS-JB 834)		
	Pruebas		
	Hallazgos		
PRUEBAS DE CUMPLIMIENTO Y SUSTANCIACIÓN			
	Evaluación del Riesgo	Entrevista	Cuestionario
	Riesgo Inherente y Residual		Registros de Observación.
	Probabilidad e Impacto		
	Mapa de Riesgos (Impacto Probabilidad)		
	Respuestas a los riesgos		
	Asignación de riesgos a los procesos de negocio		
	Evaluación de posibles respuestas		
	Prevención		
	Reducción		
	Gestión Compartida		
	Aceptación		
APLICACIÓN DE CONTROLES			
	Controles existentes	Encuesta	Cuestionario
	Aplicación de Controles		
	Políticas y Procedimientos		
3.1.1.6 comunicación de resultados			
	Emisión de Resultados y Comunicación	Elaboración de informes	Documento
	Informe		

3.1.1.1. Cobertura de la Auditoría

Objetivos de la Auditoría

- ✓ Determinar el cumplimiento y la substanciación los riesgos operativos tecnológicos enunciados en la norma JB 834 de la Superintendencia de Bancos y Seguros como factor de la eficiencia y productividad de la COAC Alianza del Valle.

3.1.1.2 Alcance de la auditoría

La auditoría está orientada a examinar los riesgos tecnológicos más relevantes que enuncia la norma SBS - JB 834, realizando pruebas de cumplimiento y substanciación de los riesgos donde el impacto afecte la cadena de valor del negocio.

Las pruebas de cumplimiento se identificarán los controles clave que deben probarse, realizando pruebas de confiabilidad, prevención de riesgos y adherencia a las políticas y procedimientos de la organización.

En las pruebas de substanciación se aplicarán procedimientos detallados de análisis de datos donde los controles sean débiles y el impacto sea alto.

3.1.1.3 Comprensión del negocio a ser auditado

Ubicación geográfica y económica

Gráfico 2: Ubicación COAC Alianza del Valle

Fuente: COAC Alianza del Valle

La Cooperativa de Ahorro y Crédito Alianza del Valle Ltda., Cooperativa Financiera controla por la Superintendencia de Economía Popular y Solidaria, nace el 26 de mayo de 1970, producto del pensamiento de 13 jóvenes visionarios, quienes acogiéndose a la Reforma Agraria empezaban a vivir independientemente y generar ingresos, factor que motivó a asociarse para promover el ahorro y crédito, buscando el progreso de la comunidad en el campo financiero, social, educativo y cultural.

La finalidad de la cooperativa se orienta a satisfacer las necesidades económicas y sociales de los sectores productivos que no tienen acceso al Sistema Financiero tradicional apoyando con su gestión a la pequeña, mediana empresa, a la solución de la microempresa y vivienda, administrando sus recursos de acuerdo a normas de prudencia y solvencia financiera, proyectando una imagen de confiabilidad a través de servicios financieros ágiles y oportunos con un enfoque social. La Casa matriz está ubicada en el Valle de los Chillos Chaupitena vía antigua Conocoto, Amaguaña como indica en el Gráfico 1.

Alianza del Valle, actualmente realiza sus operaciones en los cantones: Quito, Mejía y Rumiñahui de la provincia del Pichincha, su matriz se ubica en el barrio Chaupitena en la parroquia Amaguaña; mantiene una sucursal en la zona norte de la ciudad de Quito, el Inca, y en la parte sur operan las oficinas de Chillogallo, Conocoto, Amaguaña, Sucursal Mayor, La Colón, Guamaní, en el cantón Mejía operan la agencia Machachi y la agencia Sangolquí en el cantón Rumiñahui.

Productos y Servicios financieros

Productos financieros

La Cooperativa Alianza del Valle, ofrece productos y servicios financieros a clientes y socios dentro de su nicho de mercado que es la provincia de Pichincha.

Dentro de los productos financieros, tenemos el ahorro y crédito.

En ahorro: Ahorro a la vista y depósitos a plazo fijo

En crédito: Encontramos las siguientes modalidades y sujetos de crédito:

De consumo.- Personas naturales, con necesidad de financiamiento con destino abierto, cuya fuente de pago provenga de los ingresos como asalariado o rentista.

De microempresa.- Personas naturales o jurídicas no asalariados y/o informales, dedicados a actividades productivas comercialización o prestación de servicios a pequeña escala.

De vivienda.- Personas naturales que requieran de financiamiento para la adquisición construcción, reparación, remodelación y mejoramiento de la vivienda propia.

Comercial.- Son operaciones de crédito dirigidas a pequeñas y medianas empresas cuyas ventas anuales sean iguales a superiores a 100.000 dólares. Forman parte de este segmento las operaciones dirigidas a personas naturales que ejercen su trabajo como profesionales en libre ejercicio y registran un nivel de ingresos totales anuales por servicios prestados dentro de una actividad

profesional igual o superiores a 40.000 dólares.

La institución ha logrado ubicarse en el sexto lugar del Ranking de Cooperativas de Ahorro y Crédito del Ecuador, como se observa en el siguiente cuadro.

Tabla 5: Resultados financieros

ENTIDADES	30/11/2012 $	30/11/2012 %	31/12/2012 $	31/12/2012 %	31/12/2012 POS.
JARDIN AZUAYO	4.516,37	8,43	4.663,55	8,85	1
29 DE OCTUBRE	3.474,65	6,48	4.133,10	7,85	2
SAN FRANCISCO	3.421,15	6,38	4.107,17	7,80	3
JUVENTUD ECUATORIANA PROGRESISTA	3.623,30	6,76	3.687,16	7,00	4
CACPECO	3.565,17	6,65	3.536,74	6,71	5
ALIANZA DEL VALLE	**2.642,08**	**4,93**	**2.897,89**	**5,50**	**6**
OSCUS	3.004,23	5,61	2.766,27	5,25	7
COOPROGRESO	2.252,39	4,20	2.307,92	4,38	8
EL SAGRARIO	2.084,97	3,89	2.287,52	4,34	9
TULCAN	2.034,16	3,80	2.266,59	4,30	10
23 DE JULIO	1.944,45	3,63	2.109,20	4,00	11

Fuente: COAC Alianza del Valle

En la actualidad son 100.553 socios/clientes que confían en la Cooperativa Alianza del Valle Ltda. y acceden a productos crediticios y demás servicios con

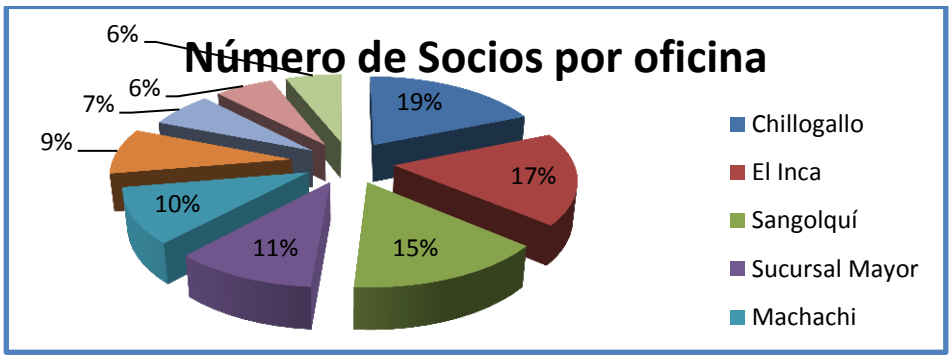
los que cuenta la institución, distribuidas de la siguiente manera. (Memoria COAC Alianza del Valle 2011, 2011)

Tabla 6: Número de socios COAC Alianza del Valle

OFICINA	NUMERO DE SOCIOS
Chillogallo	18.831
El Inca	17.545
Sangolquí	15.099
Sucursal Mayor	10.772
Machachi	10.451
Guamaní	8.766
Conocoto	6.828
La Colón	6.250
Amaguaña	6.009
SUMA	100.551

Fuente: COAC Alianza del Valle

Gráfico 3: Número de socios por oficina



Fuente: COAC. Alianza del Valle

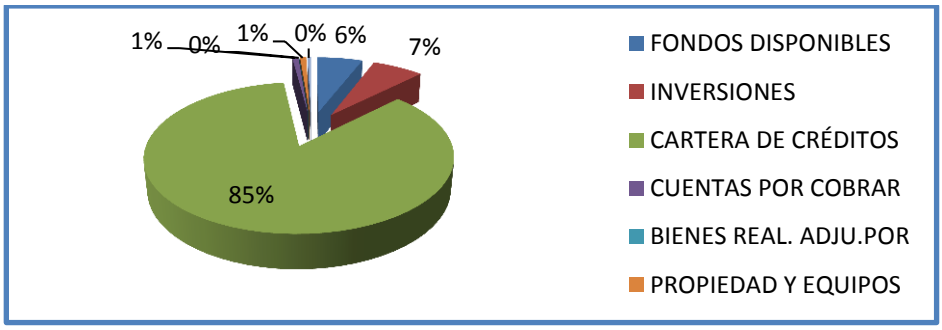
La Cooperativa Alianza del Valle alcanzó un saldo a diciembre de 2012 de 97,676,500.08 USD de sus activos, en las cuentas contables más importantes.

Tabla 7: Captaciones 2012

CUENTA	VALOR
TOTAL DE ACTIVOS	97.676.500,08
FONDOS DISPONIBLES	5.739.115,89
INVERSIONES	6.459.791,33
CARTERA DE CRÉDITOS	83.458.155,45
CUENTAS POR COBRAR	775.004,14
BIENES REAL. ADJU.POR	15.900,00
PROPIEDAD Y EQUIPOS	770.818,23
OTROS ACTIVOS	457.715,04

Fuente: COAC Alianza del Valle

Gráfico 4: Valor de activos



Fuente: COAC Alianza del Valle

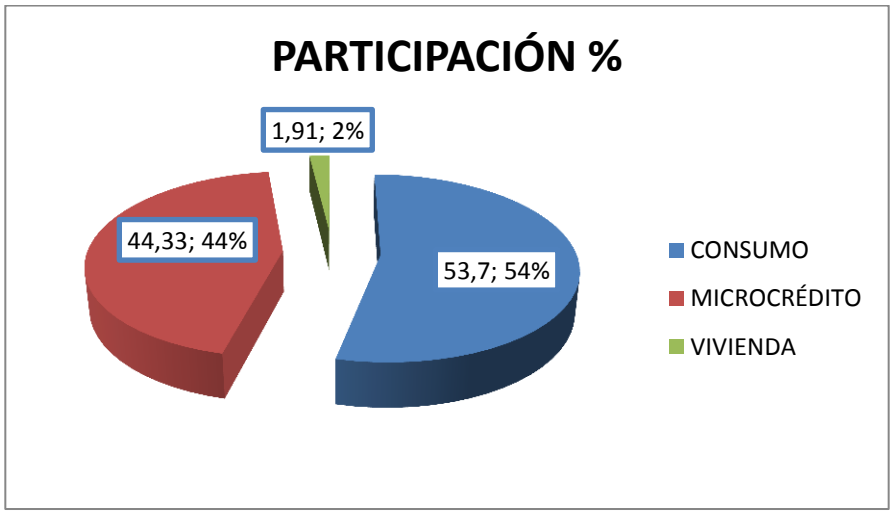
En lo referente a la composición de la cartera bruta de crédito, los segmentos más representativitos son:

Tabla 8: Segmentos

SEGMENTOS	PARTICIPACIÓN %
CONSUMO	53,70
MICROCRÉDITO	44,33
VIVIENDA	1,91

Fuente: COAC Alianza del Valle

Gráfico 5: Segmento de captación



Fuente: COAC Alianza del Valle

En cuanto a las oficinas operativas, las que han alcanzado mayores niveles de crecimiento en cartera de crédito a diciembre de 2011 son:

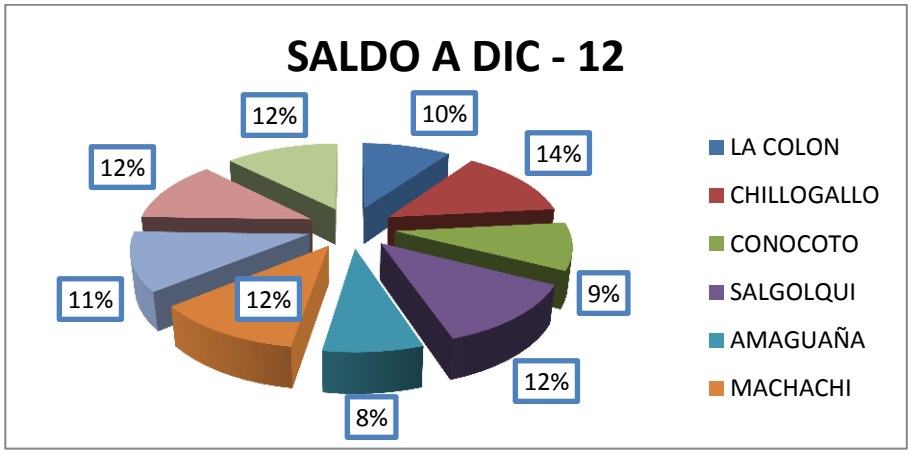
Cartera de créditos por oficinas operativas

Tabla 9: Cartera de créditos por oficinas

OFICINA	SALDO A DIC - 12
LA COLON	8.156.511,00
CHILLOGALLO	11.313.762,00
CONOCOTO	7.647.470,00
SALGOLQUI	10.308.949,00
AMAGUAÑA	6.401.780,00
MACHACHI	9.665.724,00
GUAMANI	9.503.124,00
EL INCA	10.082.748,00
SUC MAYOR	10.378.189,00

Fuente: COAC Alianza del Valle

Gráfico 6: Cartera de Crédito por oficina



Fuente: COAC Alianza del Valle

Obligaciones al público por oficinas operativas

Tabla 10: Obligaciones por oficina

OFICINA	SALDO A DIC - 11
CONOCOTO	4.042.522,00
CHILLOGALLO	9.292.460,00
AMAGUAÑA	4.574.782,00
MACHACHI	5.917.266,00
GUAMANI	4.518.387,00
COLON	4.382.722,00
SALGOLQUI	9.583.469,00
EL INCA	9.714.633,00
SUC MAYOR	14.671.016,00

Fuente: COAC Alianza del Valle

Gráfico 7: Obligaciones con el público

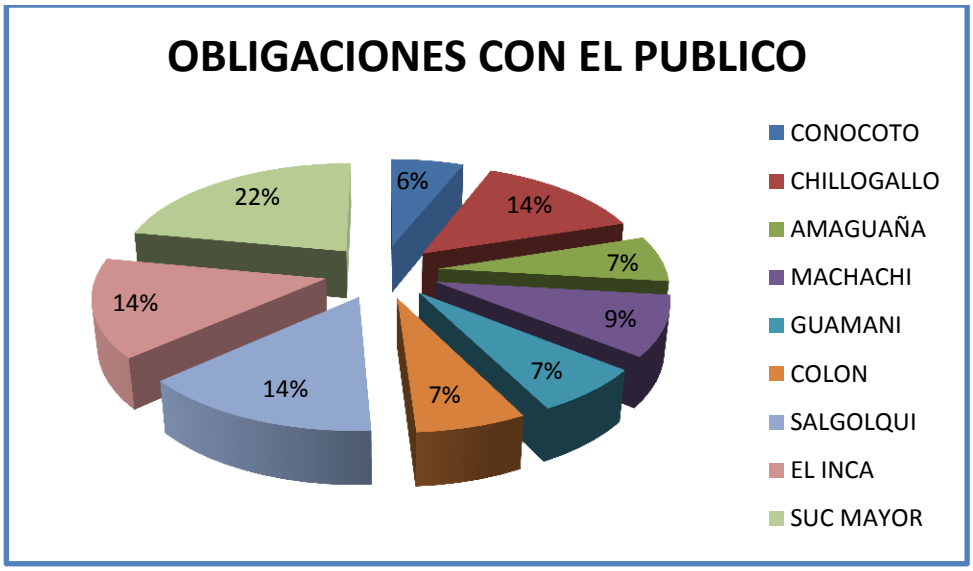


Gráfico 8: Obligaciones con el público

Fuente: COAC Alianza del Valle

Servicios financieros

La cooperativa brinda a sus clientes y socios servicios como:

Cajeros Automáticos (ATM's).- que están implementados en cada una de sus oficinas operativas, permitiendo transaccionar con tarjetas y hacer sus retiros.

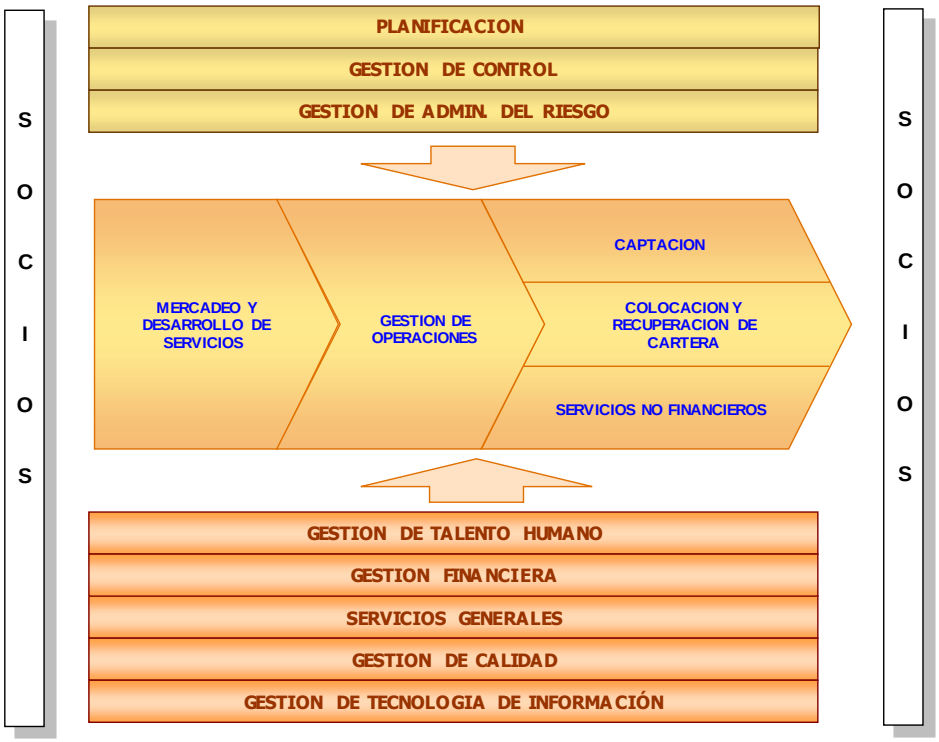
Pago directo.- Permite a los socios realizar transacciones por la web con sistema de trasferencias entre la cooperativa y un grupo de bancos y cooperativas.

Pago de servicios básicos.- Canal electrónico en convenio estratégico que permite hacer pagos de servicios como, agua, luz, matricula vehicular, tarjetas de créditos, impuestos prediales.

Procesos de Negocio (Cadena de Valor)

El Diagrama de Flujo de Proceso contenido en la sección brinda una descripción de la interacción entre los procesos de nuestro Sistema de Gestión de la Calidad.

Gráfico 9: Cadena de valor COAC Alianza del Valle

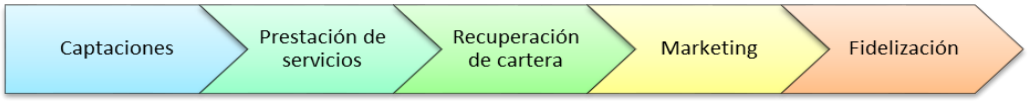


Fuente: COAC Alianza del Valle

Como podemos observar en el Gráfico No. 9 de la cadena de valor constan los procesos macros como son los Procesos Estratégicos, Procesos Productivos y de Apoyo. Inmersos en estos procesos macros se encuentran todos los departamentos que de una u otra forma interactúan unos con otros durante toda la gestión de servicio crediticio.

Procesos productivos: hacen referencia a los Procesos de la Cadena de Valor de la cooperativa y tienen impacto en el cliente creando valor para éste. Son las actividades esenciales de la institución, su razón de ser.

Gráfico 10: Cadena Procesos Productivo



Fuente: COAC Alianza del Valle

Procesos estratégicos:

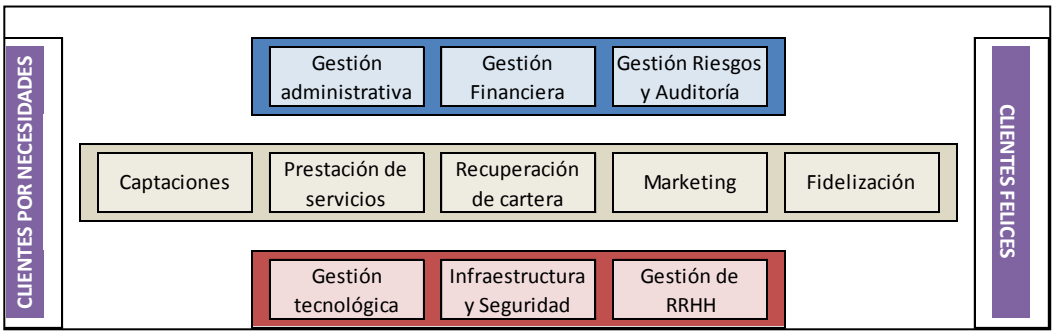
Los procesos estratégicos tiene que ver directamente con la Gestión o Administración de la Cooperativa, incluye: Gestión institucional, Gestión de Riesgos, Gestión de procesos y Gestión Institucional.

3.1.1.4 Comprensión de los procesos de negocio

El Mapa de Procesos de la COAC. Alianza del Valle, es la representación gráfica de los procesos de ésta y de sus interrelaciones, ofrece una visión general del sistema de gestión. En él se representan los procesos que componen el sistema así como sus interrelaciones.

Hay que clasificar los procesos, preparar un modelo de proceso para la empresa y prepara la documentación de los procesos.

Gráfico 11: Mapa de proceso



Fuente: COAC Alianza del Valle

Modelo de Negocios

El modelo de negocio que maneja la cooperativa está basado en cuatro pilares fundamentales:

Modelo de portafolio.- Se caracteriza por la diversidad equilibrada en términos de geografía, negocios y clientes.

Modelo de negocios.- está centrado en el cliente y socios, basados en una relación a corto y mediano plazo, en la intermediación financiera brindando productos y servicios financieros apoyándose en su cadena de valor y sus procesos de apoyo, gobernantes y estratégicos, su tamaño y escala le ha permitido acometer un importante crecimiento en su cartera de crédito, portafolio de inversiones.

Modelo de gestión.- basado en la toma de decisiones bajo principios de prudencia financiera que se ve reflejada en la gestión de riesgos de crédito,

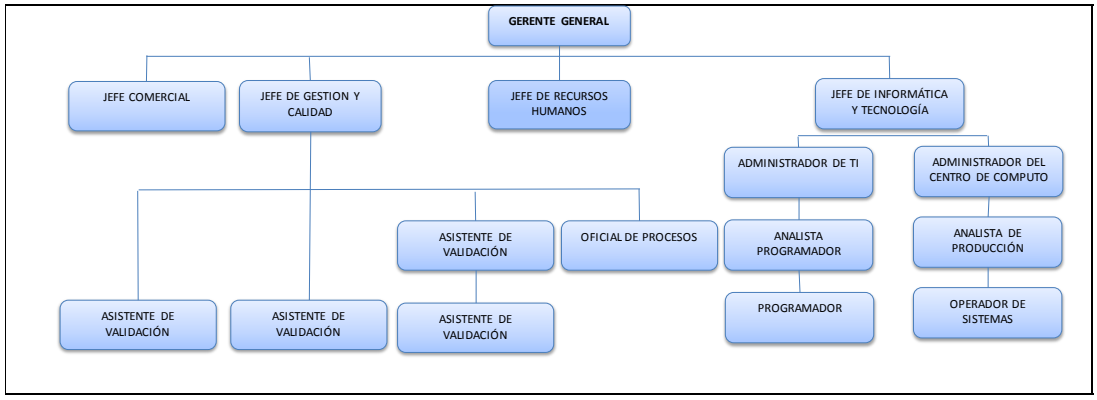
gestión de capital; y la anticipación está reflejada en el liderazgo para la toma de decisiones que anticipen a los cambios relevantes en el entorno.

Modelo de gobierno.- basado en la integridad, la prudencia, la trasparencia que genera valor a sus clientes y/o socios, esto se complementa con el cumplimiento de normativa y sistemas de buen gobierno cooperativo.

La combinación de estos cuatro elementos hace que la cooperativa genere una fuerte ventaja competitiva, fidelidad, fortaleza estructural, crecimiento sostenido.

Estructura orgánica

Gráfico 12: Estructura organizacional



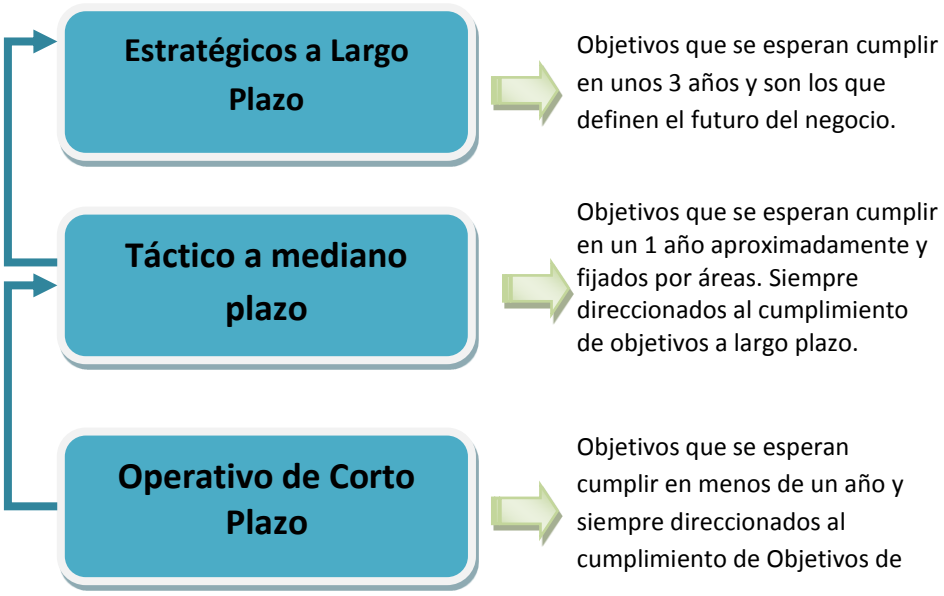
Fuente: COAC Alianza del Valle

Objetivos de la organización

Los objetivos de la Alianza del Valle se clasifican en largo, mediano y corto plazo, de acuerdo al plazo de ejecución, además clasificados en cada una de

las perspectivas del Cuadro de Mando Integral, como se observa el Gráfico Objetivos Organizacionales.

Gráfico 13: Objetivos organizacionales



Fuente: COAC Alianza del Valle

Objetivos operativos

Los principios institucionales buscan impulsar la gestión de intermediación financiera fortaleciendo la filosofía cooperativista, se sustentan en la propuesta universal de los principios cooperativos.

Tabla 11: Objetivos operativos

PERSPECTIVA	TIPO	OBJETIVO
CLIENTE	**LP**	**Mejorar la fidelidad y sentido de pertenencia del asociado**
	MP	Mejorar el posicionamiento y nivel de uso en el mercado de cobertura
	CP	Generar una ventaja competitiva basada en la implementación de la cultura de servicio al asociado con valor agregado y responsabilidad social.
FINANCIERA	**LP**	Salvaguardar una Gestión Financiera eficiente y eficaz que fortalezca la solidez, maximización de rentabilidad y permanencia en el tiempo de la Cooperativa
	MP	Fortalecer la capitalización del patimonio técnico de la Cooperativa e incrementar las fuentes de fondo interno.
	CP	Mejorar el sistema de generación de información financiera para la adecuada toma de decisiones.

Fuente: COAC Alianza del Valle

Objetivos Estratégicos

Tabla 12: Objetivos Estratégicos

OAL	OMP	OCP
Contar con un sistema fuerte en prevención de lavado de activos y de gestión de riesgos		Detectar de manera inmediata y oportuna las operaciones y transacciones que no están acorde con el perfil financiero del socio y cliente.
	Fortalecer los conocimientos en la prevención de lavado de activos, administración de riesgos y control interno	Concientizar a los directivos, funcionarios y empleados sobre sus responsabilidades dentro de la organización.
Contar con una base de datos que permita detectar deficiencias en el sistema de control, con el objeto de establecer estrategias eficientes y cumplir con las recomendaciones de los entes de control.		Conseguir una actualización del 30% de información personal y financiera de los socios/clientes activos
Alcanzar los 200 millones en activos		Obtener la calificación de operación de la SEPS
	Mejorar la cobertura de la cartera en riesgo	Reducir la cartera en riesgo

Fuente: COAC Alianza del Valle

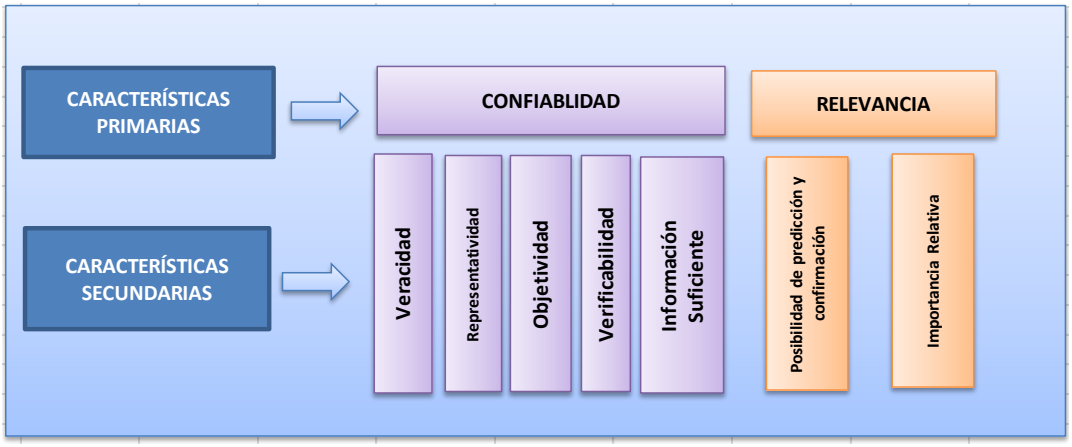
3.1.1.5 Reportes confiables

La confiabilidad y relevancia son las características que se deben considerar a la hora de generar reportes en cada uno de los departamentos.

El propósito de confiabilidad se enfoca a lograr que los usuarios tengan una misma interpretación básica de la información.

Los reportes reflejan la realidad económica y organizacional del negocio y con el mínimo grado de error, de tal forma que brinde seguridad a los usuarios, en el siguiente cuadro se describen las características de los reportes confiables.

Gráfico 14: Criterios de confiabilidad de los reportes



Fuente: COAC Alianza del Valle

Con el fin de conocer el grado de confiabilidad de los reportes generados por la cooperativa. Aplicamos el siguiente instrumento de evaluación, considerando los criterios de confiabilidad y los diversos departamentos de la institución.

Tabla 13: Aplicación de criterios de confiabilidad de los reportes

	CONFIABILIDAD					RELEVANCIA	
DEPARTAMENTO	Veracidad	Representatvidad	Objetvidad	Verificabilidad	Información Suficiente	Posibilidad de predicción	Importacia Relativa
Gerencia General	MA	MA	MA	MA	MA	A	N
Comercialización	A	MA	MA	A	A	MA	N
Gestión y Calidad	MA	A	MA	A	A	MA	N
Talento Humano	A	A	MA	A	MA	A	N
Informática y Tecnología	MA	A	MA	MA	MA	N	A
Financiero	MA	MA	MA	MA	MA	MA	N
Riesgos	MA	MA	MA	A	MA	MA	N
Cumplimiento	A	MA	A	A	A	A	N

MD= Muy en desacuerdo
D= Desacuerdo
N= Neutral
A= De Acuerdo
MA= Muy de acuerdo

Fuente: COAC. Alianza del Valle

De lo aplicado podemos deducir que la mayoría de los departamentos manejan con cierta aceptabilidad los reportes a su cargo, faltando trabajar en la importancia relevante, pues muchos de ellos son redundantes y podría integrarse interdepartamentalmente para dar mayor agilidad a los procesos.

3.1.1.6 Cumplimiento (Normas internas y Externas)
Riesgo operativo

Según el Capítulo V de las NORMAS GENERALES PARA LA APLICACIÓN DE LA LEY GENERAL DE INSTITUCIONES DEL SISTEMA FINANCIERO TITULO X.- DE LA GESTION Y ADMINISTRACION DE RIESGOS Las disposiciones de esta norma son aplicables a las instituciones financieras públicas y privadas, al Banco Central del Ecuador, a las compañías

de arrendamiento mercantil, a las compañías emisoras y administradoras de tarjetas de crédito y a las corporaciones de desarrollo de mercado secundario de hipotecas, cuyo control compete a la Superintendencia de Bancos y Seguros.

La SECCIÓN II.- FACTORES DEL RIESGO OPERATIVO ARTÍCULO 4. Con el propósito de que se minimice la probabilidad de incurrir en pérdidas financieras atribuibles al riesgo operativo, deben ser adecuadamente administrados los siguientes aspectos, los cuales se interrelacionan entre sí:

Procesos.- Para garantizar la optimización de los recursos y la estandarización de las actividades, las instituciones controladas deben contar con procesos definidos de conformidad con la estrategia y las políticas adoptadas.

Personas. El capital humano debe ser identificado de forma adecuada, e identificar apropiadamente las fallas o insuficiencias asociadas al factor “personas”, tales como: falta de personal adecuado, negligencia, error humano, nepotismo de conformidad con las disposiciones legales vigentes, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros.

Tecnología de información.- Las instituciones controladas deben contar con la tecnología de información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio y lograr que la información, inclusive

aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas, procesos y procedimientos que aseguren una adecuada planificación y administración de la tecnología de información.

Eventos externos.- En la administración del riesgo operativo, las instituciones controladas deben considerar la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos a su control, tales como: fallas en los servicios públicos, ocurrencia de desastres naturales, atentados y otros actos delictivos, los cuales pudieran alterar el desarrollo normal de sus actividades. Para el efecto, deben contar con planes de contingencia y de continuidad del negocio.

3.1.1.7 Planeación estratégica y documentos relacionados

El plan estratégico es un documento en el que los responsables de una organización (empresarial, institucional, no gubernamental, deportiva,...) reflejan cual será la estrategia a seguir por su compañía en el medio plazo, para alcanzar la visión planteado. En el caso de la Cooperativa Alianza del Valle, se considera los siguientes elementos:

Misión

Valores

Principios

Ejes de estratégicos

Plan de negocios

Estrategia de negocios

Acciones a seguir

Objetivos. Estrategias de acción

Fase II: Ejecución de la auditoría

3.1.2.1. Ambiente Interno

Declaración del código de ética

La misión y la filosofía del cooperativismo nos presentan el sustento cultural para la creación e implementación de la guía de nuestra conducta ética, la misma que nace a partir de las leyes, normas, políticas, procedimientos y reglamentos vigentes en la institución. El código de ética está ligado a la razón de ser como organización y a nuestro compromiso con la sociedad.

A continuación analizamos su estructura:

Tabla 14: Evaluación de la estructura del código de ética

Evaluación de la estructura del código de ética		
SECCIÓN	**CONTENIDO**	**EVALUACIÓN**
Carta de la Gerencia General y el Consejo de Administración	* Presenta el mensaje de Gerencia General sobre la importancia de la integridad y ética para la Cooperativa.	NO
	* Presenta su propósito y forma de uso.	SI
Objetivos y Filosofía	Se considera:	
	Su cultura	SI
	Su negocio y sector	SI
	Sus ubicaciones geográficas nacionales e internacionales	NO
	Compromiso con el liderazgo ético	SI
Incompatibilidades	Establece normas y proporciona pautas con respecto a los regalos y gastos de representación, así como a su adecuada comunicación.	SI

	Incompatibilidad en relación con el personal y otros agentes corporativos, así como aquellos actividades inversiones o intereses que podría afectar a la reputación o integridad de la entidad.	SI
Regalos y gratificaciones	Penaliza el empleo de regalos y gratificaciones, estableciendo la política de la entidad al respecto que habitualmente va mucho más allá de leyes aplicables.	SI
	Establece normas y proporciona pautas con respecto a los regalos y gastos de representación, así como a su adecuada comunicación.	SI
Transparencia	Incluye disposiciones/normas acerca del comportamiento de la empresa con la generación de informes completos y comprensibles sobre impacto social medioambiental y económico.	SI

Recursos corporativos	Incluye disposiciones/normas acerca de los recursos corporativos incluyendo la propiedad intelectual y la información de activos propios a quien pertenece y como se protege.	SI
Responsabilidad Social	Incluye el papel de la cooperativa como parte de la sociedad, incluyendo su compromiso con los derechos humanos, la preservación del medio ambiente la implicación en el desarrollo de su comunidad.	SI
Otras cuestiones relativas a la conducta	Incluye disposiciones/normas acerca de la fidelidad a las políticas establecidas en áreas específicas de actividad de la empresa, tales como:	SI

Fuente: COAC Alianza del Valle

De la evaluación a la estructura del Código de Ética se observa que:

- El Código de Ética está estructurado de tal manera que facilita el cumplimiento y la puesta en práctica del quehacer profesional con acento en la propuesta de criterios de acción y conducta.

- Es necesario incluir el mensaje de los directivos, especialmente de la Gerencia General para lograr el empoderamiento institucional y la integridad ética para la Cooperativa.
- Se debe hacer constar sus ubicaciones geográficas nacionales e internacionales, para tener un referente específico de la Cooperativa y facilite su ubicación.

Declaración de visión, misión, valores

Misión

Somos una Cooperativa de Ahorro y Crédito que ofrece a nuestros socios y clientes productos y servicios financieros de calidad con valor agregado, dentro de un marco de eficacia, eficiencia y humanismo, respaldados en el compromiso de trabajo continuo de nuestro talento humano contribuimos al mejoramiento de la calidad de vida y desarrollo económico de la comunidad.

Visión

Mantenernos como una Institución financiera sólida y competitiva a nivel regional que genera permanente valor para socios, clientes, talento humano y comunidad.

Valores:

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

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

Trabajamos con transparencia y ética cuidando siempre el bienestar de nuestros socios e institución.

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

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

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

Productos y servicios

Dentro de los productos financieros, tenemos ahorro y crédito.

En ahorro: Ahorro a la vista y depósitos a plazo fijo

En crédito: Encontramos las siguientes modalidades y sujetos de crédito:

De consumo.- Personas naturales, con necesidad de financiamiento con destino abierto, cuya fuente de pago provenga de los ingresos como asalariado o rentista.

De microempresa.- Personas naturales o jurídicas no asalariados y/o

informales, dedicados a actividades productivas comercialización o prestación de servicios a pequeña escala, cuyas ventas anuales sean de hasta 100.000 dólares.

De vivienda.- Personas naturales que requieran de financiamiento para la adquisición construcción, reparación, remodelación y mejoramiento de la vivienda propia.

Comercial.- Son operaciones de crédito dirigidas a pequeñas y medianas empresas cuyas ventas anuales sean iguales a superiores a 100.000 dólares. Forman parte de este segmento las operaciones dirigidas a personas naturales que ejercen su trabajo como profesionales en libre ejercicio y registran un nivel de ingresos totales anuales por servicios prestados dentro de una actividad profesional igual o superiores a 40.000 dólares.

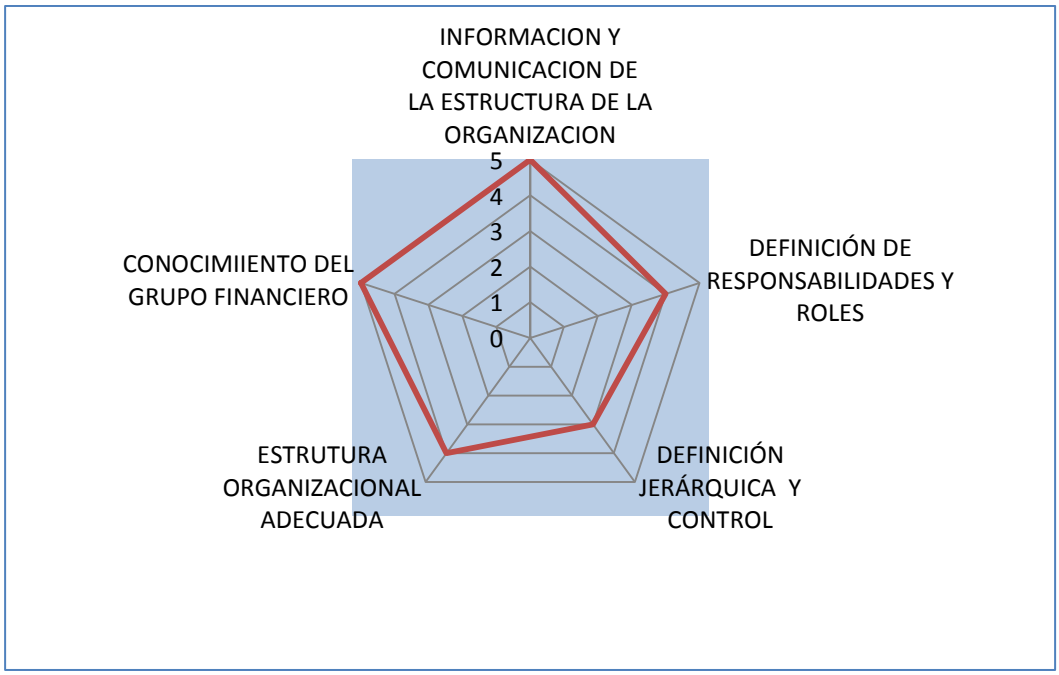
Gobierno Cooperativo

La Cooperativa de Ahorro y Crédito “Alianza del Valle” Ltda. constituida al amparo de la Ley Orgánica de Economía Popular y Solidaria y del Sector Financiero Popular y Solidario vigente en el Ecuador, ha iniciado un proceso con el fin de implementar y promover las mejores prácticas de Buen Gobierno Corporativo como parte de su gestión integral, y aplicación en los principios universales del cooperativismo.

El código de Buen Gobierno busca garantizar y acrecentar la confianza de los socios, la comunidad y demás interesados en la cooperativa, como parte de los objetivos institucionales.

A continuación se detalla la evaluación al Buen Gobierno, utilizando el método de ruta crítica y un gráfico radial para visualizar el área que requiere mayor atención.

Gráfico 15: Gráfico radial del gobierno cooperativo



Fuente: COAC Alianza del Valle

El gráfico indica una debilidad considerable en DEFINICIÓN DE JERARQUÍA Y CONTROL y se fortalece en INFORMACIÓN Y COMUNICACIÓN, Conocimiento del grupo y Estructura organizacional, por lo que es necesario establecer acciones tendientes a mejorar la debilidad identificada**.**

Control Interno

El control interno es un proceso integral que es aplicado por la máxima autoridad, la dirección y el personal de la institución, que suministra seguridad razonable para el logro de los objetivos institucionales y la protección de los recursos privados. Los componentes que constituyen su marco de referencia del control interno son: el ambiente de control, la evaluación de riesgos, las actividades de control, los sistemas de información y comunicación y el seguimiento.

Distribución Jerárquica del Control Interno

Gráfico 16: Jerarquía del control interno

Fuente: Cobit

Entorno de TI en un Contexto de Negocio

Los riesgos de tecnología de la información son un elemento del conglomerado de riesgos a los que está expuesta la organización. Otros de los riesgos a los que una organización se enfrenta pueden ser riesgos estratégicos, riesgos reputacional, riesgos legales, riesgos ambientales, riesgos de mercado, riesgos de crédito, riesgos operativos y riesgos de cumplimiento. En las cooperativas por resolución de la SBS se instó, los riesgos relacionados con TI y que se consideran un componente de riesgo operativo. Un ejemplo de lo mencionado es en el sector financiero en el marco de Basilea II. Sin embargo, el riesgo estratégico de TI tiene inferencia en el componente financiero. Lo mismo se aplica para el riesgo de crédito, donde las políticas a veces deficientes y pobres en cuanto a seguridad de la información se refiere, conllevan a menores calificaciones de crédito. Por esta razón, es mejor no describir los riesgos de Tecnología de la Información como una dependencia jerárquica en una de las categorías de riesgo, tal como se muestra en el gráfico 13 jerarquías de control interno.

3.1.2.2 Establecimiento de objetivos

Área a ser Auditada

Se realizará Auditoria a la Gestión de Riesgos y específicamente al Área de Tecnología, revisando brevemente las otras áreas.

Procesos

Objetivos de Control*:*

✓ Identificar los procesos con los que cuenta bajo los parámetros definidos en la norma de Riesgo Operativo

✓ Determinar la existencia de procedimientos para la administración de procesos

Situación Actual

✓ Cuenta con un inventario y/o mapa de procesos de toda la entidad

✓ Los procesos están agrupados en: gobernantes, productivos y de soporte

✓ Tiene identificadas las líneas de negocios de acuerdo con el segmento de mercado objetivo y asignados los procesos a cada una de ellas.

✓ Ha identificado los procesos críticos propios de la entidad y los provistos por terceros, relacionándolos con las "líneas de negocio".

✓ Los procesos están debidamente diseñados (detalle del tipo de procesos, secuencia lógica de las actividades, responsables y áreas involucradas.

✓ Cuenta con políticas y procedimientos de difusión y comunicación de los procesos a nivel de toda la organización.

Observaciones

✓ No cuenta con un manual de procedimientos formalizado para el diseño, levantamiento y descripción de los procesos

✓ No existe una adecuada separación de funciones que evite fraudes, errores, omisiones u otros eventos de riesgo operativo.

✓ No cuenta con políticas y procedimientos de medición y gestión de procesos, es decir: indicadores de gestión.

✓ No existen políticas y procedimientos para el seguimiento permanente de la gestión de los procesos que permita la actualización y mejora continua de los mismos.

Personas

Objetivos de Control*:*

Determinar la definición de procedimientos para la Administración del Capital Humano bajo los parámetros definidos en la norma de riesgo operativo.

Situación Actual

✓ Los procesos de incorporación, permanencia y desvinculación están ajustados a las disposiciones legales garantizando condiciones laborales idóneas.

✓ Cuenta con un Código de Ética / Código de Conducta formalmente establecido y difundido en todos los niveles de la entidad.

Observaciones

✓ La administración del capital humano no cuenta con políticas y procedimientos para cada uno de los procesos de incorporación, permanencia y desvinculación del personal.

✓ No cuenta con análisis para la determinación del personal necesario y las competencias idóneas para el desempeño de cada puesto.

✓ No cuenta con una base de datos actualizada de su capital humano (número de personas, formación académica y experiencia, fechas de selección, reclutamiento y selección, eventos de capacitación, cargos que ha desempeñado, evaluaciones de desempeño, fechas y causas de separación del personal, entre otras).

Eventos externos

Objetivos de Control*:*

Definir un esquema formal para la administración del riesgo operativo acorde con la administración integral de riesgos, que permita: identificar, medir, controlar y monitorear las exposiciones al mencionado riesgo.

Situación Actual

✓ Cuenta con niveles de control formalmente establecidos y validados periódicamente para asegurar un adecuado sistema de control interno que mitigue los eventos de riesgo operativo.

Observaciones

✓ No se ha identificado formalmente por línea de negocio los eventos de riesgo operativo, agrupados por tipo de evento y, las fallas o insuficiencias en los factores de riesgo operativo.

✓ No se ha conformado bases de datos centralizados, suficientes y de calidad con información sobre los eventos de riesgo operativo y de fallas o insuficiencias en los factores de riesgo operativo conforme lo dispuesto en la

resolución JB-2005-834; que sean alimentadas de acuerdo con procedimientos formales que involucran a toda la organización.

✓ Auditoría Interna no realiza periódicamente pruebas orientadas a determinar el cumplimiento de las políticas, procedimientos y requerimientos regulatorios para la administración del riesgo operativo.

✓ No cuenta con esquemas organizados de reportes para la gestión del riesgo operativo.

Tecnológicos (SBS JB 834)

El Art. 4 del Capítulo 5, establece la necesidad de que las instituciones establezcan formalmente políticas, procesos y procedimientos que aseguren una adecuada planificación y administración de la tecnología de información.

Dichas políticas, procesos y procedimientos se referirán a:

4.3.1 Con el objeto de garantizar que la **administración de la tecnología de información soporte adecuadamente los requerimientos** de operación actuales y futuros de la entidad, las instituciones controladas deben contar al menos con lo siguiente:

4.3.2 Con el objeto de garantizar que **las operaciones de tecnología de información satisfagan los requerimientos de la entidad**, las instituciones controladas deben contar al menos con lo siguiente:

4.3.3 Con el objeto de garantizar que los recursos y servicios provistos por terceros, se administren con base en responsabilidades claramente definidas y estén sometidas a un **monitoreo de su eficiencia y efectividad.**

4.3.4 Con el objeto de garantizar que el sistema de administración de seguridad satisfaga las necesidades de la entidad para **salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas**. Las instituciones controladas deben contar al menos con lo siguiente:

4.3.5 Con el objeto de garantizar la **continuidad de las operaciones**, las instituciones controladas deben contar al menos con lo siguiente:

4.3.6 Con el objeto de garantizar que el **proceso de adquisición, desarrollo, implementación y mantenimiento de las aplicaciones satisfagan los objetivos del negocio**, las instituciones controladas deben contar al menos con lo siguiente:

4.3.7 Con el objeto de garantizar que la **infraestructura tecnológica** que soporta las operaciones, **sea administrada, monitoreada y documentada de forma adecuada, las instituciones** controladas deberán contar con políticas y procedimientos que permitan la adecuada administración, monitoreo y documentación de las bases de datos, redes de datos, software de base y hardware.

3.1.2.3 Identificación de Objetivos y Riesgos

Riesgos Identificados en TI

La cooperativa tiene procedimientos que facilita la identificación de los riesgos de las fuentes que tiene la institución, de esta forma han identificado si existen debilidades o amenazas en dichos fuentes.

Como es un proceso sistémico tiene definido los objetivos en su planeación estratégica y en los factores clave del negocio para alcanzar las metas y revisar cuales son las debilidades de los proyectos y las amenazas a las que enfrenta. La cooperativa tiene registros de su modelo de identificación de riesgos como herramienta fundamental el análisis FODA, en particular los puntos débiles y las amenazas, ofrecerán una visión de los riesgos a los que enfrenta la cooperativa.

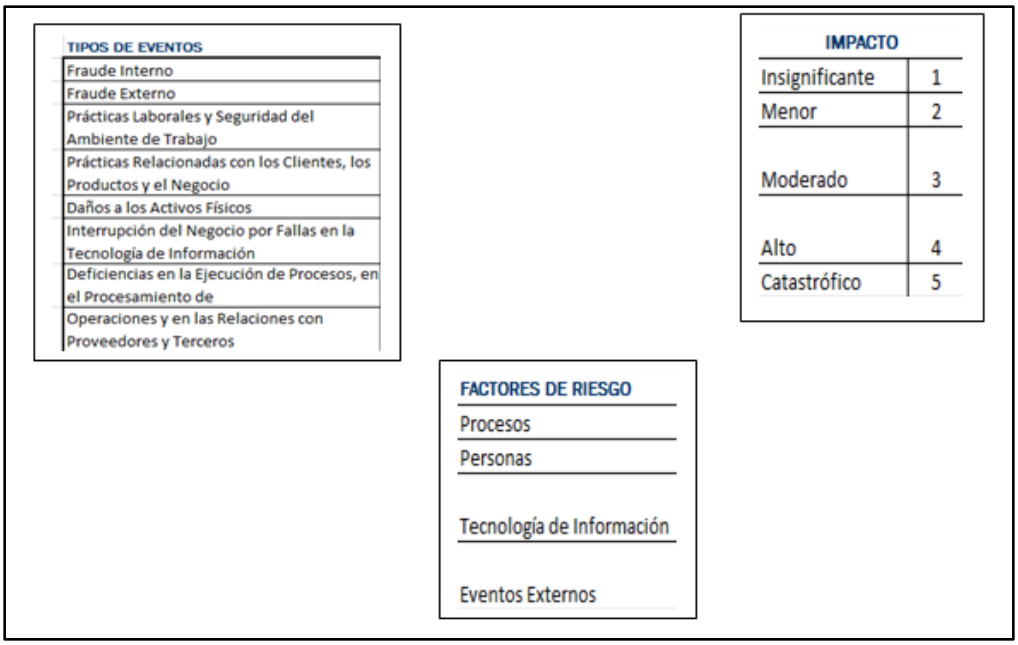
A continuación se esquematiza como la cooperativa Alianza del Valle identifica los riesgos, considerando que es un procedimiento que lo ha estado ejecutando para luego elaborar la matriz de riesgos y darles los pesos correspondientes.

Los riesgos operativos están relacionados con la habilidad de la cooperativa para convertir la estrategia elegida en planes concretos, mediante la asignación eficaz de recursos, en la Figura siguiente se expone dicho procedimiento.

Gráfico 17: Procedimiento de identificación de riesgos

En el proceso de auditoría a la cooperativa, se encontró que cuenta con una matriz de riesgos en función de proceso, macro proceso, proceso, describiendo el riesgo, tipo de evento, factor de riesgo y calificándolo en función de impacto probabilidad, severidad, levantada en función a un análisis previo de procesos críticos que afectan a la cadena de valor, calificada en función de la metodología de juicio de expertos (Delphi), la valoración se identifican a continuación en función de los procesos de TI.

Gráfico 18: Método de evaluación de matrices de riesgo



TIPOS DE EVENTOS
Fraude Interno
Fraude Externo
Prácticas Laborales y Seguridad del Ambiente de Trabajo
Prácticas Relacionadas con los Clientes, los Productos y el Negocio
Daños a los Activos Físicos
Interrupción del Negocio por Fallas en la Tecnología de Información
Deficiencias en la Ejecución de Procesos, en el Procesamiento de
Operaciones y en las Relaciones con Proveedores y Terceros

IMPACTO	
Insignificante	1
Menor	2
Moderado	3
Alto	4
Catastrófico	5

FACTORES DE RIESGO
Procesos
Personas
Tecnología de Información
Eventos Externos

Tabla 15: Matriz de identificación de riesgos

Tipo de Proceso	Macroproceso	Proceso	Subproceso	Responsable del Proceso	Descripción del Riesgo	Tipos de Eventos	Factores de riesgo	Impacto	Impacto	Probabilidad	Probabilidad
APOYO	GESTIÓN DE INFORMÁTICA Y TECNOLOGÍA	GESTIÓN DE INFORMÁTICA Y TECNOLOGÍA	PLANIFICACIÓN Y CONTROL	Jefe de Informática y Tecnología	Uso de claves compartidas	Prácticas Relacionadas con los Clientes, los Productos y el Negocio	Personas	3	Moderado	3	Moderada
				Jefe de Informática y Tecnología	Instalación de software no autorizado	Prácticas Relacionadas con los Clientes, los Productos y el Negocio	Personas	3	Moderado	2	Baja
				Jefe de Informática y Tecnología	Destrucción de información mal intencionad	Fraude Interno	Personas	4	Alto	2	Baja
				Jefe de Informática y Tecnología	Modificación no autorizada de software	Prácticas Relacionadas con los Clientes, los Productos y el Negocio	Personas	3	Moderado	1	Muy baja
				Jefe de Informática y Tecnología	Concentración de funciones	Prácticas Laborales y Seguridad del Ambiente de Trabajo	Procesos	3	Moderado	1	Muy baja
				Jefe de Informática y Tecnología	Robo de software institucional	Fraude Interno	Personas	2	Menor	2	Baja
				Jefe de Informática y Tecnología	No se han formalizado los SLA´s, UC, OLA, con proveedores internos y exexternos	en el Procesamiento de Operaciones y en las Relaciones con Proveedores y Terceros	Procesos	2	Menor	2	Baja
				Jefe de Informática y Tecnología	institución no se encuentran registrados en el Instituto Ecuatoriano de la Propiedad Intelectual	Deficiencias en la Ejecución de Procesos, en el Procesamiento de Operaciones y en las Relaciones con Proveedores y Terceros	Procesos	3	Moderado	3	Moderada
				Jefe de Informática y Tecnología	Deterioro de los respaldos de información	Deficiencias en la Ejecución de Procesos, en el Procesamiento de Operaciones y en las Relaciones con Proveedores y Terceros	Eventos Exter	3	Moderado	2	Baja
				Jefe de Informática y Tecnología	Abuso de información privilegiada	Fraude Interno	Personas	3	Moderado	1	Muy baja
				Jefe de Informática y Tecnología	Instalación de hardware no autorizado en los equipos de computo	Prácticas Relacionadas con los Clientes, los Productos y el Negocio	Personas	2	Menor	1	Muy baja
				Jefe de Informática y Tecnología	Sustracción de hardware	Fraude Interno	Personas	2	Menor	3	Moderada
				Jefe de Informática y Tecnología	Las instalaciones donde se encuentran los backups de los equipos de computo son vulnerables	Deficiencias en la Ejecución de Procesos, en el Procesamiento de Operaciones y en las Relaciones con Proveedores y Terceros	Eventos Exter	3	Moderado	3	Moderada
				Jefe de Informática y Tecnología	Códigos de acceso de personas desvinculadas se mantiene activo	Deficiencias en la Ejecución de Procesos, en el Procesamiento de Operaciones y en las Relaciones con Proveedores y Terceros	Procesos	3	Moderado	1	Muy baja
				Jefe de Informática y Tecnología	No se lleva un registro de las personas que acceden a áreas restringidas	Deficiencias en la Ejecución de Procesos, en el Procesamiento de Operaciones y en las Relaciones con Proveedores y Terceros	Procesos	2	Menor	2	Baja

				Jefe de Informática y Tecnología	condiciones físicas idóneas para mitigación de eventos externos tales como: incendios, inundaciones,	Deficiencias en la Ejecución de Procesos, en el Procesamiento de Operaciones y en las Relaciones con Proveedores y Terceros	Eventos Exter	4	Alto	1	Muy baja
				Jefe de Informática y Tecnología	No se cuenta con personal entrenado para enfrentar eventos externos	Prácticas Laborales y Seguridad del Ambiente de Trabajo	Personas	2	Menor	3	Moderada
				Jefe de Informática y Tecnología	Politica de Seguridad de la información se encuentra desactualizada y no ha sido socializada	Deficiencias en la Ejecución de Procesos, en el Procesamiento de Operaciones y en las Relaciones con Proveedores y Terceros	Procesos	2	Menor	3	Moderada
			EXPLOTACIÓN Y SOPORTE IT	Administrador Centro de computo	El acceso al Data Center tiene seguridades	Deficiencias en la Ejecución de Procesos, en el Procesamiento de Operaciones y en las Relaciones con Proveedores y Terceros	Tecnología de Información	2	Menor	3	Moderada
				Administrador Centro de computo	No se cuenta con procedimientos estandarizados del control de cambios a nivel de hardware y software	Deficiencias en la Ejecución de Procesos, en el Procesamiento de Operaciones y en las Relaciones con Proveedores y Terceros	Procesos	1	Insignifica	4	Alta
				Administrador Centro de computo	No se cuenta con herramientas de monitoreo de las comunicaciones	Interrupción del Negocio por Fallas en la Tecnología de Información	de Información	2	Menor	3	Moderada
				Administrador Centro de computo	No se cuenta con una red LAN no segmentada (plana)	Interrupción del Negocio por Fallas en la Tecnología de Información	de Información	3	Moderado	4	Alta
				Administrador Centro de computo	Data Center limitado en espacio físico y dis	Deficiencias en la Ejecución de Procesos, en el Procesamiento de Operaciones y en las Relaciones con Proveedores y Terceros	Tecnología de Información	3	Moderado	4	Alta
				Administrador Centro de computo	Sitio alterno con minimas adecuaciones lóg	Deficiencias en la Ejecución de Procesos, en el Procesamiento de Operaciones y en las Relaciones con Proveedores y Terceros	Tecnología de Información	4	Alto	4	Alta
				Administrador Centro de computo	El personal tiene escasa capacitación especializada en eventos externos	Prácticas Laborales y Seguridad del Ambiente de Trabajo	Personas	2	Menor	3	Moderada
				Administrador Centro de computo	Monopolio de la empresa de soporte y mant	Prácticas Relacionadas con los Clientes, los Productos y el Negocio	Eventos Exter	3	Moderado	3	Moderada
				Administrador Centro de computo	Ataques externos a las redes	Fraude Externo	Eventos Exter	4	Alto	2	Baja
				Administrador Centro de computo	Manipulación de la configuración de Equipo	Deficiencias en la Ejecución de Procesos, en el Procesamiento de Operaciones y en las Relaciones con Proveedores y Terceros	Personas	3	Moderado	2	Baja
				Administrador Centro de computo	Denegación del servicio de red	Interrupción del Negocio por Fallas en la Tecnología de Información	Tecnología d	3	Moderado	1	Muy baja
				Administrador Centro de computo	Personal clave no disponible	Prácticas Laborales y Seguridad del Ambiente de Trabajo	Personas	3	Moderado	1	Muy baja

		GESTIÓN Y DESARROLLO DE SOFTWAR	Administrador de TI	Cambio de prioridades de proyectos informáticos sin planificación	en el Procesamiento de Operaciones y en las Relaciones con Proveedores y Terceros	Procesos	2	Menor	3	Moderada
			Administrador de TI	Cambios que modifican la base de datos	Deficiencias en la Ejecución de Procesos, en el Procesamiento de Operaciones y en las Relaciones con Proveedores y Terceros	Tecnología de Información	3	Moderado	2	Baja
			Administrador de TI	Errores de mantenimiento / actualización de programas	Interrupción del Negocio por Fallas en la Tecnología de Información	Personas	3	Moderado	2	Baja
			Administrador de TI	Utilización de Software ilegal	Prácticas Relacionadas con los Clientes, los Productos y el Negocio	Procesos	2	Menor	2	Baja
			Administrador de TI	Modificaciones no autorizadas de datos	Deficiencias en la Ejecución de Procesos, en el Procesamiento de Operaciones y en las Relaciones con Proveedores y Terceros	Personas	3	Moderado	1	Muy baja
			Administrador de TI	No se cuenta con una clasificación de la información de acuerdo a su grado de confidencialidad e importancia	Deficiencias en la Ejecución de Procesos, en el Procesamiento de Operaciones y en las Relaciones con Proveedores y Terceros	Procesos	3	Moderado	3	Moderada
			Administrador de TI	Suplantación de la identidad del usuario	Fraude Interno	Personas	2	Menor	3	Moderada
			Administrador de TI	Fuga de información privilegiada	Fraude Interno	Personas	3	Moderado	3	Moderada

Fuente: COAC Alianza del Valle

Objetivo de control: Planificación y control

Riesgos

- Uso de claves compartidas
- Destrucción de información mal intencionada
- Concentración de funciones
- Códigos de acceso de personas desvinculadas se mantiene activo
- Política de Seguridad de la información se encuentra desactualizada y no ha sido socializada

Objetivo de control: Explotación y soportes del TI

Riesgos

- El acceso al Data Center tiene seguridades físicas limitadas
- No se cuenta con procedimientos estandarizados del control de cambios a nivel de hardware y software
- No se cuenta con herramientas de monitoreo de las comunicaciones
- No se cuenta con una red LAN no segmentada (plana)

- Data Center limitado en espacio físico y distribución
- Sitio alterno con mínimas adecuaciones lógicas y físicas
- El personal tiene escasa capacitación especializada en eventos externos
- Monopolio de la empresa de soporte y mantenimiento
- Ataques externos a las redes
- Denegación del servicio de red

Objetivo de control: Estructura orgánico - funcional de TI

Riesgos

- No se ha Conformado el Comité de Tecnología

Condición:	La Cooperativa Alianza del Valle no cuenta con Comité de Tecnología que esté alineado al marco de trabajo de administración de riesgos de la institución.
Criterio:	El Comité de Tecnología se encarga de estrategia tecnológico de apoyo al negocio.
Causa:	Este trabajo está inmerso en las actividades que realiza el CAIR.
Efecto:	Al no existir el Comité de Tecnología tampoco se definen estrategias de apoyo al negocio.

Objetivo de control: Manual de políticas y procedimientos de tecnología de información

Riesgos

- Existe el manual de políticas y procedimientos pero no se ha difundido en todos los niveles de la organización.

Condición:	Se ha definido el manual de políticas y procedimientos pero no se ha realizado una correcta y completa difusión a todos los usuarios de cada uno de los departamentos.
Criterio:	Cooperativa Alianza del Valle se tiene elaborado el Manual de Procedimientos, el mismo que se ha difundido a gerencia y es conocido por los integrantes del Departamento de Tecnología.
Causa:	No se ha considerado necesario hacerlo a toda la institución
Efecto:	Personal bien informado redunda en la eficiencia de la aplicación de políticas y procedimientos.

Objetivo de control: Plan de entrenamiento y capacitación anual para el personal de TI.

Riesgos

- No existe plan de entrenamiento, el entrenamiento es basado en requerimientos inmediatos y no de largo plazo.

Condición:	Al momento en la Cooperativa Alianza del Valle se designa un presupuesto para capacitaciones en forma estimada.
Criterio:	Es indispensable que la Cooperativa establezco o diseñe un plan de capacitación que permita abordar los requerimientos de los empleados y disponer del presupuesto adecuado.
Causa:	Se atiende las capacitaciones según las necesidades y las oportunidades que se presenten.
Efecto:	Tener un presupuesto fijo, y organización permanente, para localizar las mejores oportunidades tanto en costo como en beneficio.

Objetivo de control: Acuerdos escritos que describan los niveles de servicio en términos cualitativos y cuantitativos y responsabilidades de ambas partes

Riesgos

- En los documentos no se describe los niveles de servicio en términos cuantitativos.

Condición:	La Cooperativa Alianza del Valle tiene acuerdos firmados como parte habilitantes en los contratos pero solo son cualitativos estos se les denomina SLA's
Criterio:	Los acuerdos firmados como parte habilitantes en contratos deben ser cualitativos y cuantitativos, para poder ejercer acciones legales.

Causa:	Por falta de cumplimiento a las recomendaciones de auditorías externas que así lo mencionan
Efecto:	Puede desencadenar en problemas legales.

Objetivo de control: Procedimientos para soporte a usuarios dentro de una función de Help Desk o Mesa de Control y Ayuda.

Riesgos

- No se ha actualizado para procedimientos para soporte a usuarios

Condición	Los procedimientos para soportes a usuarios dentro de función de Help Desk o mesa de Control, proporcionan a los usuarios un soporte efectivo.
Criterio:	Se tiene implementado una herramienta informática llama Sisayd, sin embargo no se han formalizado los procedimientos, existiendo únicamente buenas prácticas.
Causa:	Ineficiencia en la aplicación en la formalización de procedimientos.
Efecto:	Al no tener procedimientos formalizados se corre el riesgo de no tener estandarizado el soporte y los acuerdos entre usuarios, creando en confusión en la gestión de soporte.

- No existe una revisión de Procedimientos por el CAIR

Condición:	EL CAIR se encarga de la administración y gestión de riesgos integrales de la institución, por tanto es el encargado de revisar los procedimientos.
Criterio:	EL CAIR está incumpliendo las normativas de la Superintendencia de Bancos (Control y Gestión de Riesgos Integrales)
Causa:	Negligencia en el cumplimiento de las normativas.
Efecto:	La Cooperativa pueda estar sujeta a sanciones por incumplimiento de la normativa.

Objetivo de control: Verificar la existencia de procedimientos para la administración de activos de tecnología que incluyan su registro, clasificación, control y responsables de su uso y mantenimiento.

Riesgos

- Es necesario actualizar procedimientos para soporte a usuarios

Condición:	Los procedimientos para la administración para la administración de riesgos de tecnología incluir su registro, clasificación, control y responsables de su uso y mantenimiento.
Criterio:	No se ha establecido los procedimientos
Causa:	El control de adquisiciones de Activos Tecnológicos se lo ha estado realizando en base al Manual de Adquisiciones General

	de la Cooperativa.
Efecto:	No permite realizar un análisis detallado de los activos informáticos, ya que su tratamiento es diferente.

- Se necesita la revisión de Procedimientos por el CAIR

Condición:	EL CAIR se encarga de la administración y gestión de riesgos integrales de la institución, por tanto es el encargado de revisar los procedimientos.
Criterio:	EL CAIR está incumpliendo las normativas de la Superintendencia de Bancos (Control y Gestión de Riesgos Integrales)
Causa:	Negligencia en el cumplimiento de las normativas.
Efecto:	La Cooperativa pueda estar sujeta a sanciones por incumplimiento de la normativa.

Objetivo de control: Se ha definido un procedimiento formal y continuo de monitoreo sobre la prestación de servicio de terceros, con el fin de asegurar el cumplimiento de los acuerdos del contrato.

Riesgos

Revisión de Procedimientos por el CAIR

Condición:	EL CAIR se encarga de la administración y gestión de riesgos integrales de la institución, por tanto es el encargado de

	revisar los procedimientos.
Criterio:	EL CAIR está incumpliendo las normativas de la Superintendencia de Bancos (Control y Gestión de Riesgos Integrales)
Causa:	Negligencia en el cumplimiento de las normativas.
Efecto:	La Cooperativa pueda estar sujeta a sanciones por incumplimiento de la normativa.

- Aprobación del Consejo de Administración

Condición:	El Consejo de Administración, es el órgano encargado de dictar aprobar políticas institucionales.
Criterio:	No se ha dado a conocer los procedimientos para su aprobación.
Causa:	Negligencia del encargado de presentar la política.
Efecto:	Incumplimiento de normativas y aplicación informal de procedimientos.

Objetivo de Control: La entidad cuenta con políticas y procedimientos de seguridad de la información aprobadas formalmente, difundidas e implementadas; incluyendo aquellas relacionadas con servicios de transferencia y transacciones electrónicas, si aplica.

Riesgos

- No se ha realizado la difusión de políticas y procedimientos en todos los niveles de la organización.

Condición:	Las políticas y procedimientos de seguridad de la información aprobadas, difundidas e implementadas proporcionan eficiencia en la aplicación de las Tecnologías de la Información.
Criterio:	La Cooperativa cuenta con políticas y procedimientos de la información, aprobadas e implementadas pero no han sido completamente difundidas.
Causa:	No existen procedimientos de socialización efectiva, se lo hace a través de uso de repositorios y comunicación a través de correo electrónico.
Efecto:	Desconocimiento de la aplicación de procedimientos.

Objetivo de control: La entidad dispone de un plan de evaluación del desempeño del sistema de administración de la seguridad de la información que permita tomar acciones para mejorarlo.

Riesgos

- Definición de política para la revisión periódica del sistema de administración de seguridad.

Condición:	La política de revisión periódica del sistema de administración de seguridad permite gestionar las políticas de aseguramiento de los sistemas de información
Criterio:	La Cooperativa Alianza del Valle no ha definido políticas de

	administración de seguridad.
Causa:	No existe un oficial de seguridades que gestione las políticas y procedimientos de los sistemas de información.
Efecto:	Vulnerabilidad de los sistemas de información.

- Aprobación del Consejo de Administración

Condición:	El Consejo de Administración, es el órgano encargado de dictar aprobar políticas institucionales.
Criterio:	No se ha dado a conocer los procedimientos para su aprobación.
Causa:	Negligencia del encargado de presentar la política.
Efecto:	Incumplimiento de normativas y aplicación informal de procedimientos.

Objetivo de control: La entidad cuenta con un procedimiento de monitoreo para evaluar el cumplimiento de la metodología del ciclo de vida de desarrollo de sistemas

Riesgos

- Definición de procedimientos de monitoreo

Condición:	El monitoreo para evaluar el cumplimiento del ciclo de vida de desarrollo de sistemas, es necesario para evidenciar e identificar problemas que se presenten en la implementación.

Criterio:	Nos se ha definido procedimientos de monitoreo.
Causa:	Negligencia del encargado de presentar la política.
Efecto:	Incumplimiento de normativas y aplicación informal de procedimientos.

- Revisión de procedimientos por el CAIR

Condición:	EL CAIR se encarga de la administración y gestión de riesgos integrales de la institución, por tanto es el encargado de revisar los procedimientos.
Criterio:	EL CAIR está incumpliendo las normativas de la Superintendencia de Bancos (Control y Gestión de Riesgos Integrales)
Causa:	Negligencia en el cumplimiento de las normativas.
Efecto:	La Cooperativa pueda estar sujeta a sanciones por incumplimiento de la normativa.

- Aprobación del Consejo de Administración

.Condición:	El Consejo de Administración, es el órgano encargado de dictar aprobar políticas institucionales.
Criterio:	No se ha dado a conocer los procedimientos para su aprobación.
Causa:	Negligencia del encargado de presentar la política.
Efecto:	Incumplimiento de normativas y aplicación informal de procedimientos.

Objetivo de control: La entidad tiene procedimientos formales para administración de versiones que garanticen el registro, evaluación y autorización de los cambios previos a su implantación y la revisión posterior contra los resultados planeados.

Riesgos

- Se ha elaborado los procedimiento y se aplican pero falta la revisión de procedimientos por el CAIR

Condición:	EL CAIR se encarga de la administración y gestión de riesgos integrales de la institución, por tanto es el encargado de revisar los procedimientos.
Criterio:	EL CAIR está incumpliendo las normativas de la Superintendencia de Bancos (Control y Gestión de Riesgos Integrales)
Causa:	Negligencia en el cumplimiento de las normativas.
Efecto:	La Cooperativa pueda estar sujeta a sanciones por incumplimiento de la normativa.

- Falta la aprobación del Consejo de Administración

Condición:	El Consejo de Administración, es el órgano encargado de dictar aprobar políticas institucionales.
Criterio:	No se ha dado a conocer los procedimientos para su aprobación.

Causa:	Negligencia del encargado de presentar la política.
Efecto:	Incumplimiento de normativas y aplicación informal de procedimientos.

Objetivo de control: Políticas y procedimientos formales para la administración del desempeño y la capacidad de los recursos de TI

- No se han definido de procedimientos para la administración del desempeño y la capacidad de los recursos de TI.

Condición:	Los procedimientos para la administración del desempeño y la capacidad de los recursos de TI inciden en la eficiencia de adquisiciones.
Criterio:	La Cooperativa tiene procedimientos formalizados aprobados, pero no se hace el seguimiento ni monitoreo.
Causa:	Negligencia en el seguimiento de los procedimientos.
Efecto:	El seguimiento a los procedimiento debe aplicarse para realizar actualizaciones y medir la proyección del negocio y evitar un sobre dimensionamiento en adquisiciones

- Falta la revisión de procedimientos por el CAIR

Condición:	EL CAIR se encarga de la administración y gestión de riesgos integrales de la institución, por tanto es el encargado de revisar los procedimientos.
Criterio:	EL CAIR está incumpliendo las normativas de la

	Superintendencia de Bancos (Control y Gestión de Riesgos Integrales)
Causa:	Negligencia en el cumplimiento de las normativas.
Efecto:	La Cooperativa pueda estar sujeta a sanciones por incumplimiento de la normativa.

Objetivo de control: Políticas y procedimientos de administración de configuraciones de la infraestructura tecnológica.

Riesgos

- Falta la definición de procedimientos para la administración de configuraciones de la infraestructura tecnológica

Condición:	La SBS establece la obligación de formalizar procedimientos para la administración de la infraestructura tecnológica.
Criterio:	Actualmente se tiene procedimientos formalizados y aprobados para la Administración de configuraciones de la infraestructura tecnológica aprobados, pero no se hace el seguimiento ni monitoreo
Causa:	Negligencia en la administración de procedimientos.
Efecto:	El seguimiento debe aplicarse para realizar actualizaciones y medir la proyección del negocio.

- Se debe realizar la revisión de procedimientos por el CAIR

Condición:	EL CAIR se encarga de la administración y gestión de riesgos integrales de la institución, por tanto es el encargado de revisar los procedimientos.
Criterio:	EL CAIR está incumpliendo las normativas de la Superintendencia de Bancos (Control y Gestión de Riesgos Integrales)
Causa:	Negligencia en el cumplimiento de las normativas.
Efecto:	La Cooperativa pueda estar sujeta a sanciones por incumplimiento de la normativa.

Objetivo de control: Políticas formales y controles para detectar y evitar la instalación de software no autorizado o no licenciado, así como instalar y actualizar periódicamente aplicaciones de detección y eliminación de virus informático y demás software malicioso

Riesgos

- Falta adquirir software para el control de aplicativos no autorizados.

Condición:	El software de control de aplicaciones impide la utilización de software no autorizado
Criterio:	Se tiene implementado reglas de seguridad vía firewall, e implementado Active director y que han permitido realizar los controles, pero no se ha formalizado.

Causa:	Negligencia o desconocimiento de la norma
Efecto:	Vulnerabilidad en la intrusión de usuarios externos que afecten a los sistemas de información.

- No se ha definido políticas para el control y monitoreo del software que utiliza la institución.

Condición:	Las políticas de monitorio en los manuales de explotación deben ser aprobadas por el Consejo de Administración para formalizar su aplicación.
Criterio:	Existen políticas de monitoreo en los manuales de explotación y soporte; se han realizado actualizaciones, falta ser aprobadas por el consejo de administración, falta la formalización causando como efecto la aplicación formal.
Causa	Por negligencia
Efecto:	Falta de formalidad en la aplicación de los procedimientos.

Riesgo Aceptado

El riesgo aceptado se expresa en términos cuantitativos y cualitativos, en la Cooperativa se lo hace cualitativamente, calificando de Alto, Moderado, Bajo, evidenciándose en la matriz donde se valora los riesgos; sin considerar el nivel de riesgo máximo aceptado, como también la tolerancia al riesgo, permitiendo tener un nivel aceptable de las desviaciones en el logro de los objetivos, en la tabla 16 se observa la medición en forma cualitativa y según explicación se la elabora aplicando el método Delphi.

Tabla 16: Matriz de riesgo aceptado

Tipo de Proceso	Macroproceso	Proceso	Subproceso	Responsable del Proceso	Descripción del Riesgo	Riesgo
			PLANIFICACIÓN Y CONTROL	Jefe de Informática y Tecnología	Uso de claves compartidas	Moderado
				Jefe de Informática y Tecnología	Instalación de software no autorizado	Moderado
				Jefe de Informática y Tecnología	Destrucción de información mal intencionada	Alto
				Jefe de Informática y Tecnología	Modificación no autorizada de software	Moderado
				Jefe de Informática y Tecnología	Concentración de funciones	Moderado
				Jefe de Informática y Tecnología	Robo de software institucional	Bajo
				Jefe de Informática y Tecnología	No se han formalizado los SLA´s, UC, OLA, con proveedores internos y exexternos	Bajo
				Jefe de Informática y Tecnología	Los programas desarrollados por la institución no se encuentran registrados en el Instituto Ecuatoriano de la Propiedad Intelectual	Alto
				Jefe de Informática y Tecnología	Deterioro de los respaldos de información	Bajo
				Jefe de Informática y Tecnología	Abuso de información privilegiada	Moderado
				Jefe de Informática y Tecnología	Instalación de hardware no autorizado en los equipos de computo	Bajo
				Jefe de Informática y Tecnología	Sustracción de hardware	Bajo
				Jefe de Informática y Tecnología	Las instalaciones donde se encuentran los backups de los equipos de computo son vulnerables	Bajo
APOYO	GESTIÓN DE INFORMÁTICA Y TECNOLOGÍA	GESTIÓN DE INFORMÁTICA Y TECNOLOGÍA		Jefe de Informática y Tecnología	No se lleva un registro de las personas que acceden a áreas restringidas	Moderado
				Jefe de Informática y Tecnología	El centro de computo no reúne condiciones físicas idóneas para mitigación de eventos externos tales como: incendios, inundaciones, terremotos, plagas, etc.	Bajo
				Jefe de Informática y Tecnología	No se cuenta con personal entrenado para enfrentar eventos externos	Alto
				Jefe de Informática y Tecnología	Politica de Seguridad de la información se encuentra desactualizada y no ha sido socializada	Moderado
			EXPLOTACIÓN Y SOPORTE IT	Administrador Centro de computo	El acceso al Data Center tiene seguridades físicas limitadas	Alto
				Administrador Centro de computo	No se cuenta con procedimientos estandarizados del control de cambios a nivel de hardware y software	Moderado
				Administrador Centro de computo	No se cuenta con herramientas de monitoreo de las comunicaciones	Alto
				Administrador Centro de computo	No se cuenta con una red LAN no segmentada (plana)	Alto
				Administrador Centro de computo	Data Center limitado en espacio físico y distribución	Alto
				Administrador Centro de computo	Sitio alterno con minimas adecuaciones lógicas y físicas	Moderado
				Administrador Centro de com	El personal tiene escasa capacitación especializada en eventos externos	Moderado
				Administrador Centro de computo	Monopolio de la empresa de soporte y mantenimiento	Alto
				Administrador Centro de computo	Ataques externos a las redes	Alto
				Administrador Centro de computo	Manipulación de la configuración de Equipos	Moderado
				Administrador Centro de computo	Denegación del servicio de red	Moderado
				Administrador Centro de computo	Personal clave no disponible	Moderado
			GESTIÓN Y DESARROLLO DE SOFTWARE	Administrador de TI	informáticos sin planificación	Bajo
				Administrador de TI	Cambios de requerimientos que precisan modificaciones en la codificación	Moderado
				Administrador de TI	Errores de mantenimiento / actualización de programas	Bajo
				Administrador de TI	Utilización de Software ilegal	Alto
				Administrador de TI	Modificaciones no autorizadas de datos	Alto
				Administrador de TI	No se cuenta con una clasificación de la información de acuerdo a su grado de confidencialidad e importancia	Bajo
				Administrador de TI	Suplantación de la identidad del usuario	Moderado
				Administrador de TI	Fuga de información privilegiada	Moderado
				Administrador de TI	El tiempo requerido para desarrollar el proceso de requerimientos es subestimado	Bajo

Tolerancia al Riesgo

La tolerancia al riesgo son los niveles aceptables de desviación relativa a la consecución de objetivos, operar dentro de las tolerancias al riesgo proporciona a la dirección una mayor confianza en que la entidad permanece dentro de su riesgo aceptado, que proporciona la seguridad que la entidad alcanzará sus objetivos.

La Cooperativa no ha establecido un nivel de tolerancia al riesgo, donde se haga un cruce entre los objetivos con riesgo aceptado para determinar la tolerancia al riesgo y que no se den desviaciones en los objetivos corporativos.

Matriz de objetivos y Riesgos Críticos

Tabla 17: Matriz de objetivos y riesgos críticos

Macroproceso	Proceso	Descripción del Riesgo
GESTIÓN DE INFORMÁTICA Y TECNOLOGIA	Planficación estratégica de Tecnología de la Información	No se ha Conformado el Comité de Tecnología
		Existe el manual de políticas y procedimientos pero no se ha difundido en todos los niveles de la organización
		Existe entrenamiento basado en requerimientos inmediatos y no de largo plazo.
	Procedimientos para garantizar que las operaciones de TI satisfagan los requerimientos de la entidad	En los documentos no se describe los niveles de servicio en términos cuantitativos
		No se han establecido procedimientos para soporte a usuarios dentro de una función de Help Desk o Mesa de Control y Ayuda
	Administración de servicios tecnológicos provistos por terceros	Se ha definido un procedimiento formal y continuo de monitoreo sobre la prestación de servicio de terceros, pero no ha sido revisados por el CAIR.
		A pesar de existir los procedimientos no han sido Aprobados por el Consejo de Administración
	Sistema de administración de seguridad de la información	La entidad cuenta con políticas y procedimientos de seguridad de la información aprobadas formalmente, que no han sido difundidas en todos los nivles de la organización
		No se ha definición de política para la revisión periódica del sistema de administración de seguridad.
		Aprobación del Consejo de Administración

	Políticas y procedimientos para la adquisición, desarrollo, implementación y mantenimiento de las aplicaciones.	La entidad no cuenta con un procedimiento de monitoreo para evaluar el cumplimiento de la metodología del ciclo de vida de desarrollo de sistemas.
		La entidad no tiene procedimientos formales para administración de versiones que garanticen el registro, evaluación y autorización de los cambios previos a su implantación y la revisión posterior contra los resultados planeados
		Revisión de procedimientos por el CAIR
	Políticas y procedimientos administración, monitoreo y documentación de la infraestructura tecnológica?	No se han definido de procedimientos para la administración del desempeño y la capacidad de los recursos de TI.
		Falta la definición de procedimientos para la administración de configuraciones de la infraestructura tecnológica
		Falta adquirir software para el control de aplicativos no autorizados.
		No se ha definido políticas para el control y monitoreo del software que utiliza la institución

Fuente: COAC Alianza del Valle

Para la evaluación de la matriz utilizamos los siguientes criterios

Tabla 18: Criterios de evaluación de los riesgos

Nivel	RANGO	FRECUENCIA
5	Muy Alta	*Probabilidad que ocurra al menos una vez al mes*
4	Alta	*Probabilidad que no ocurra en un mes pero si al menos una vez en tres meses*
3	Moderada	*Probabilidad que no ocurra en tres meses pero si al menos una vez en seis meses*
2	Baja	*Probabilidad que no ocurra en seis meses pero si al menos una vez en un año*
1	Muy Baja	*Probabilidad que ocurra en un período mayor a un año*

SEVERIDAD			RIESGO	DESCRIPCIÓN
4	Crítico		*Riesgo Inaceptable*	Requiere acciones inmediatas.
3	Alto		*Riesgo Importante*	Atención de directivos. Planes de seguimiento.
2	Moderado		*Riesgo Tolerante*	Procedimientos normales de control y reportados a las líneas de supervisión
1	Bajo		*Riesgo aceptable*	Se administra con procedimientos rutinarios, no requiere ninguna acción.

Fuente: COAC Alianza del Valle

3.1.2.4 Evaluación del Riesgo

Riesgo Inherente y Residual

El riesgo inherente es aquél al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

El riesgo residual es aquél que permanece después de que la dirección desarrolle sus respuestas a los riesgos, refleja el riesgo remanente una vez se han implantado de manera eficaz las acciones planificadas por la dirección para mitigar el riesgo inherente.

Estas acciones pueden incluir las estrategias de diversificación relativas a las concentraciones de clientes, productos u otras, las políticas y procedimientos que establezcan límites, autorizaciones y otros protocolos, el personal de supervisión para revisar medidas de rendimiento e implantar acciones al respecto o la automatización de criterios para estandarizar y acelerar la toma de decisiones recurrentes y la aprobación de transacciones. Además, pueden reducir la probabilidad de ocurrencia de un posible evento, su impacto o ambos conceptos a la vez.

Probabilidad e Impacto

Mapa de Riesgos (Impacto Probabilidad)

Al estimar la probabilidad e impacto de posibles eventos, ya sea sobre la base del efecto inherente o residual, se debe aplicar alguna forma de medición.

A modo de ejemplo, se pueden establecer cuatro tipos generales de medida: Nominal, ordinal, de intervalo y de proporción.

Medición nominal

Es la forma más sencilla de medición e implica el agrupamiento de eventos por categorías, tales como la económica, tecnológica o medioambiental.

Riesgo Inherente

Matriz de Riesgo Inherente

Tabla 19: Matriz de distribución de control

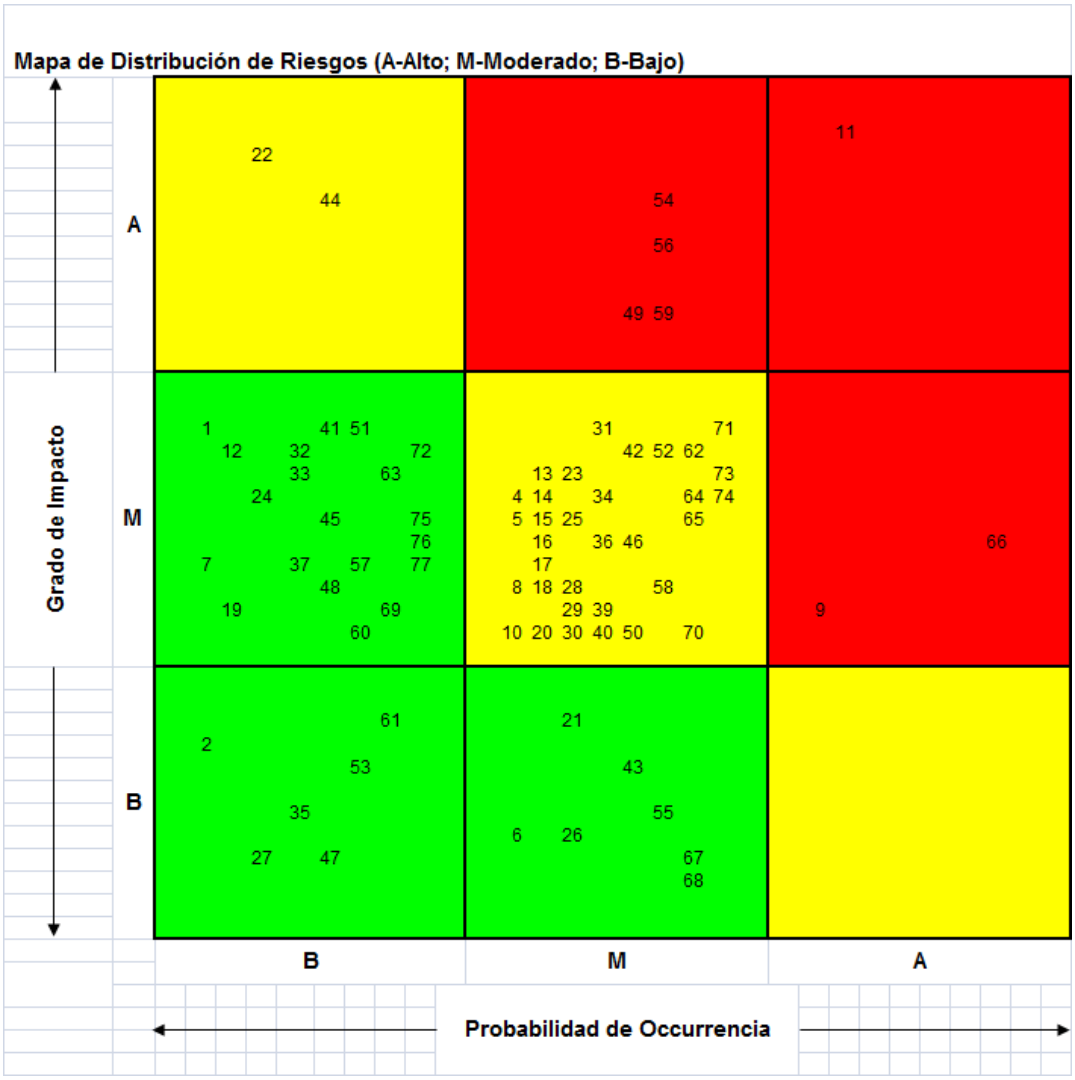
	Riesgo	Sub-categoría	Significancia	Impacto	Probabilidad	Distribución de Control
1	Competencia	Riesgos de Ambiente Interno	1	2	1	1
2	Deseos de los Socios		1	1	1	1
3	Innovación Tecnológica		2	3	2	1
4	Sensibilidad		1	2	2	2
5	Relaciones con los Socios		1	2	2	2
6	Disponibilidad de Capital		1	1	2	1
7	Soberano / Político		2	2	1	2
8	Legal		1	2	2	2
9	Regulatorio		2	2	3	2
10	Empresa		1	2	2	2
11	Mercados Financieros		2	3	3	2
12	Pérdida Catastrófica		3	2	1	2
13	Satisfacción al cliente	Riesgos de Procesos	4	2	2	2
14	Recursos Humanos		4	2	2	2
15	Capital de conocimiento		4	2	2	1
16	Desarrollo de Productos		4	2	2	2
17	Eficiencia		4	2	2	2
18	Capacidad		4	2	2	1
19	Brecha de Performance		2	2	1	1
20	Tiempo de Ciclo		4	2	2	1

21	Abastecimiento		2	1	2	2
22	Efectividad de Canales		3	3	1	2
23	Alianzas		4	2	2	1
24	Cumplimiento		2	2	1	2
25	Interrupción		4	2	2	2
26	Falla de Productos / Servicios		2	1	2	2
27	Medio Ambiente		1	1	1	2
28	Salud y Seguridad		4	2	2	1
29	Erosión de Marca		4	2	2	2
30	Eficiencia	Riesgo de Personas	4	2	2	2
31	Capacidad		4	2	2	2
32	Rotación		2	2	1	1
33	Ambiete Laboral		2	2	1	1
34	Competencia		4	2	2	3
35	Nepotismo		1	1	1	1
36	Incorporación		4	2	2	2
37	Permanencia		2	2	1	1
39	Desvinculación		4	2	2	2
40	Ética		4	2	2	1
41	Experiencia		2	2	1	2
42	Legal		4	2	2	1
43	Autoridad / Límite		2	1	2	1
44	Evaluacion de desempeño		3	3	1	2
45	Incentivos		2	2	1	1
46	Fraude		4	2	2	2
47	Robo de información		1	1	1	1
48	Relevancia	Riesgos de Tecnología de Información	2	2	1	1
49	Integridad		6	3	2	1
50	Acceso		4	2	2	1
51	Disponibilidad		2	2	1	2
52	Infraestructura		4	2	2	1
53	Fraude Gerencial		1	1	1	1
54	Fraude de Empleados / Terceros		6	3	2	2
55	Actos Ilegales		2	1	2	2
56	Uso no Autorizado		6	3	2	1
57	Reputación		2	2	1	1
58	Precio de Productos / Servicios		4	2	2	1
59	Compromiso Contractual		6	3	2	2
60	Medición Operativa		2	2	1	2

61	Alineamiento		1	1	1	1
62	Servicios Públicos	Riesgos de Eventos externos	4	2	2	2
63	Desastres Naturales		2	2	1	1
64	incumplimiento de SLAS		4	2	2	1
65	Fraude externo		4	2	2	1
66	Monopolio de proveedores		6	2	3	3
67	Fallo en Telecomunicaciones privadas		2	1	2	1
68	Asesoramiento		2	1	2	1
69	Productos informáticos defectuosos		2	2	1	2
70	Contraparte comercial		4	2	2	1
71	Distribuidores y proveedores		4	2	2	2
72	Valuación		2	2	1	1
73	Estructura Organizacional		4	2	2	1
74	Medición de Performance		4	2	2	1
75	Asignación de Recursos		2	2	1	2
76	Planeamiento		2	2	1	2
77	Ciclo de Vida		2	2	1	1

Mapa de Distribución de Riesgo Inherente

Tabla 20: Mapa de distribución de riesgo inherente de Impacto y probabilidad



Fuente: COAC Alianza del Valle

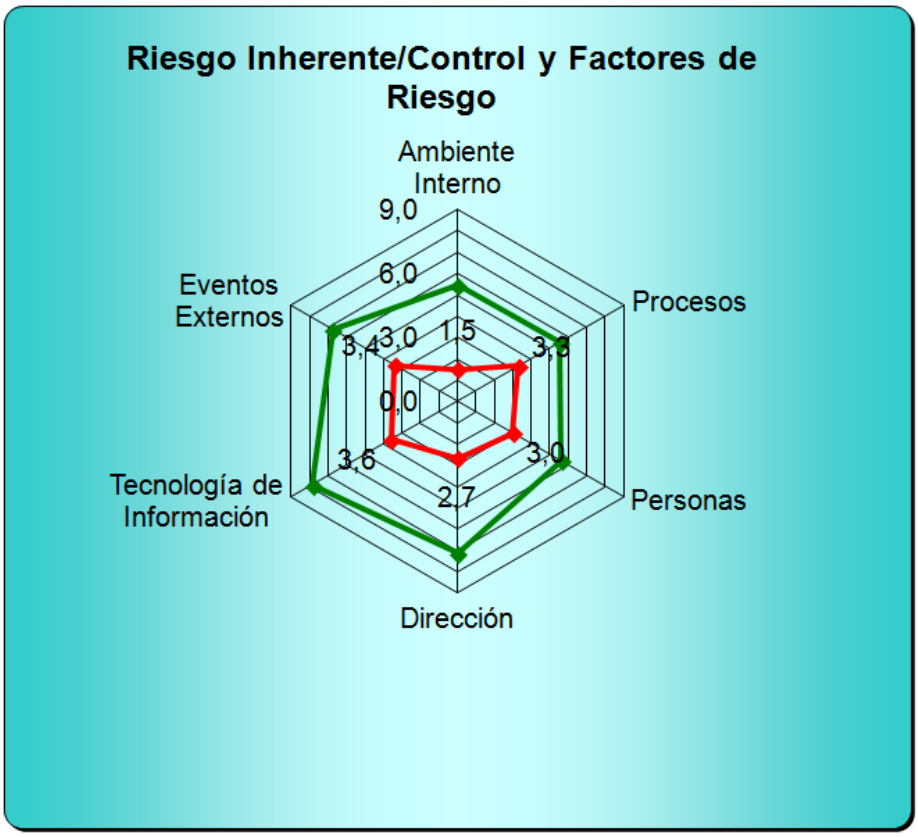
Según se observa en el mapa de riesgos inherentes la mayor concentración de riesgos está en el cuadrante de grado de impacto medio y de

ocurrencia media, los controles son aceptables, con tendencia a que la probabilidad que la vulnerabilidad se convierta en riesgo es baja pero en caso de que se materialice puede afectar a los procesos que están operando.

Gráfico 19: Riesgo inherente

Riesgo/Control y Factores de Riesgo

	Ambiente Interno	Procesos	Personas	Dirección	Tecnología de Información	Eventos Externos
Evaluación Riesgo	1,5	3,3	3,0	2,7	3,6	3,4
Evaluación Control	5,4	5,5	5,6	7,1	7,8	6,8



Fuente: COAC Alianza del Valle

En el gráfico se observa que los controles para el riego de personas son eficientes, pero el tecnológico es bajo, el riesgo en personas es bajo, sin embargo el tecnológico tanto en control como en riesgo es deficiente.

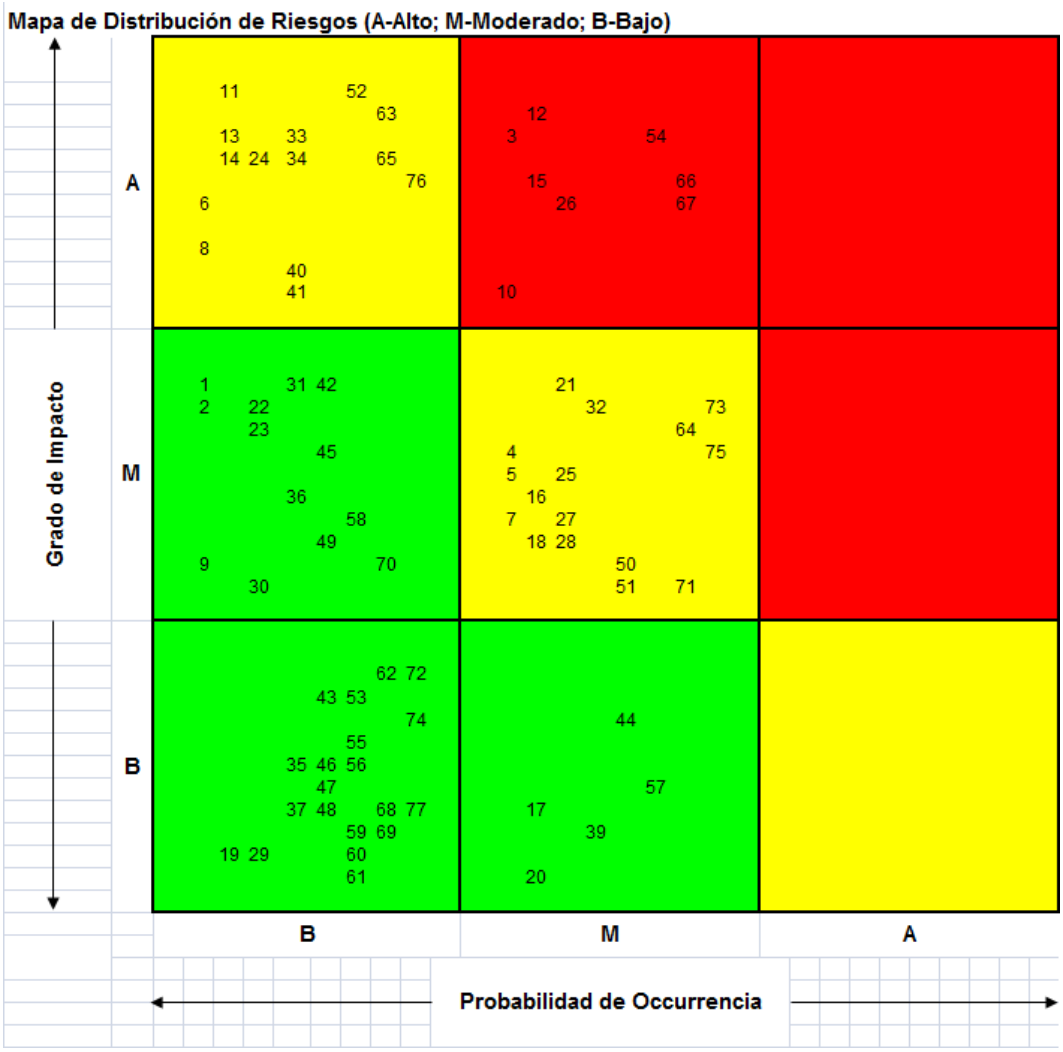
Riesgo Residual

Tabla 21: Matriz del impacto y probabilidad

	Riesgo	Facores de Riesgo	Significancia	Impacto	Probabilidad	Distribución de Control
1	Competencia	Ambiente Interno	1	2	1	1
2	Deseos de los Socios		1	1	1	1
3	Innovación Tecnológica		2	3	2	1
4	Sensibilidad		1	2	2	2
5	Relaciones con los Socios		1	2	2	2
6	Disponibilidad de Capital		1	1	2	1
7	Soberano / Político		2	2	1	2
8	Legal		1	2	2	2
9	Regulatorio		2	2	3	2
10	Empresa		1	2	2	2
11	Mercados Financieros		2	3	3	2
12	Pérdida Catastrófica		3	2	1	2
13	Satisfacción al cliente	Procesos	4	2	2	2
14	Recursos Humanos		4	2	2	2
15	Capital de conocimiento		4	2	2	1
16	Desarrollo de Productos		4	2	2	2
17	Eficiencia		4	2	2	2
18	Capacidad		4	2	2	1
19	Brecha de Performance		2	2	1	1
20	Tiempo de Ciclo		4	2	2	1
21	Abastecimiento		2	1	2	2
22	Efectividad de Canales		3	3	1	2
23	Alianzas		4	2	2	1
24	Cumplimiento		2	2	1	2
25	Interrupción		4	2	2	2
26	Falla de Productos / Servicios		2	1	2	2
27	Medio Ambiente		1	1	1	2
28	Salud y Seguridad		4	2	2	1
29	Erosión de Marca		4	2	2	2
30	Eficiencia	Personas	4	2	2	2
31	Capacidad		4	2	2	2
32	Rotación		2	2	1	1
33	Ambiete Laboral		2	2	1	1
34	Competencia		4	2	2	3
35	Nepotismo		1	1	1	1
36	Incorporación		4	2	2	2
37	Permanencia		2	2	1	1
39	Desvinculación		4	2	2	2
40	Ética		4	2	2	1
41	Experiencia		2	2	1	2
42	Legal		4	2	2	1
43	Autoridad / Límite		2	1	2	1
44	Evaluacion de desempeño		3	3	1	2
45	Incentivos		2	2	1	1
46	Fraude		4	2	2	2
47	Robo de información		1	1	1	1

48	Relevancia	Tecnología de Información	2	2	1	1
49	Integridad		6	3	2	1
50	Acceso		4	2	2	1
51	Disponibilidad		2	2	1	2
52	Infraestructura		4	2	2	1
53	Fraude Gerencial		1	1	1	1
54	Fraude de Empleados / Terceros		6	3	2	2
55	Actos Ilegales		2	1	2	2
56	Uso no Autorizado		6	3	2	1
57	Reputación		2	2	1	1
58	Precio de Productos / Servicios		4	2	2	1
59	Compromiso Contractual		6	3	2	2
60	Medición Operativa		2	2	1	2
61	Alineamiento		1	1	1	1
62	Servicios Públicos	Eventos externos	4	2	2	2
63	Desastres Naturales		2	2	1	1
64	incumplimiento de SLAS		4	2	2	1
65	Fraude externo		4	2	2	1
66	Monopolio de proveedores		6	2	3	3
67	Fallo en Telecomunicaciones privadas		2	1	2	1
68	Asesoramiento		2	1	2	1
69	Productos informáticos defectuosos		2	2	1	2
70	Contraparte comercial		4	2	2	1
71	Distribuidores y proveedores		4	2	2	2
72	Valuación		2	2	1	1
73	Estructura Organizacional		4	2	2	1
74	Medición de Performance		4	2	2	1
75	Asignación de Recursos		2	2	1	2
76	Planeamiento		2	2	1	2

Tabla 22: Matriz de distribución del riesgo



Fuente: COAC Alianza del Valle

En el mapa representa el riego residual y se observa que los controles que están en vigencia deben ser fortalecidos o proceder a una mejora ya que el impacto sigue posesionándose alto, existiendo además riesgos que son de probabilidad media pero si existe materialización el impacto es grave y se requiere planes y programas de mitigación.

3.1.2.5 Respuesta a los riesgos

Asignación de riesgos a los procesos de negocio

En este caso se asigna respuestas a los riesgos de tecnología identificados.

Tabla 23: Matriz de respuesta al riesgo

EVITAR	COMPARTIR
- Instalación de software no autorizado - Destrucción de información mal intencionada - Modificación no autorizada de software - Abuso de información privilegiada - Monopolio de la empresa de soporte y mantenimiento - Ataques externos a las redes - Manipulación de la configuración de Equipos - Cambio de prioridades de proyectos informáticos sin planificación	- Planificación estratégica de la tecnología de información, aprobada y respaldada por un procedimiento formal. - Plan operativo anual y presupuesto aprobados formalmente. - Procedimientos para la administración de incidentes y problemas incluyendo su registro, análisis y solución oportuna. - Documentación y establecimiento de procedimientos para las operaciones de tecnología de información.
REDUCIR	**ACEPTAR**
- Concentración de funciones - Robo de software institucional Deterioro de los respaldos de información -Instalación de hardware no autorizado en los equipos de computo. - Instalaciones donde se encuentran los backups vulnerables.	- Servicios de TI provistos por terceros se administran de acuerdo con las políticas institucionales de contratación de servicios. - Los contratos de servicios de TI provistos por terceros definen la propiedad de la información asi como las responsabilidades de cada parte. - La entidad ha identificado los requerimientos de seguridad relacionados con la tecnología de información y ha implementado los controles necesarios para minimizar el impacto de las vulnerabilidades e incidentes de seguridad. - La entidad cuenta con un sistema de administración de las seguridades de acceso a la información y niveles de autorización de accesos para ejecución de las funciones de procesamiento.

Fuente: COAC Alianza del Valle

Evaluación de posibles respuestas

Una vez establecidas las respuestas a los riesgos identificados, la dirección selecciona las posibles respuestas desarrollando una serie de gestiones para alinearlos con el riesgo aceptado y las tolerancias al riesgo de la entidad, la cooperativa no posee un estándar formalizado de respuesta al riesgo.

Matriz de riesgos por proceso para establecer la vinculación

La Cooperativa no ha establecido matrices para establecer la vinculación, en su defecto lo que ha elaborado es matrices de los procesos críticos.

Pruebas de cumplimiento y sustantivas

Riesgo 1: Cambios en la infraestructura tecnológica

Controles internos:	El área de Informática y Tecnología apoya en el sistema de mesa de ayuda con la herramienta SysAid.
Pruebas de cumplimiento:	Un registro formal de los cambios y cambios emergentes que se realizan en los diferentes componentes que administra y controla TI, con lo cual cuenta con un repositorio de las ultimas configuraciones y versiones de aplicativos puestos en producción.
Pruebas sustantivas:	No se registran los cambios que se realizan en el Hardware y Software corriendo el riesgo de implementar cambios sin autorización o que no son probados y aprobados formalmente, como parches, actualizaciones de firmware, etc.

Riesgo 2: Continuidad del Negocio

Controles internos:	Existe unte documento que se adjunta el procedimiento de dos servicios del negocio que son el de Depósitos con doble papeleta y eliminación de la utilización del biométrico para retiros.
Pruebas de cumplimiento:	No se ha definido e implementado un Plan de Continuidad del Negocio que involucre a toda la entidad, expone a la cooperativa a no estar preparada en caso de ocurrir un evento fortuito o desastre natural.
Pruebas sustantivas:	No se ha definido una metodología o política institucional para la administración de un Plan de Continuidad del Negocio (BCP), el documento revisado hace referencia a un plan de contingencias y recuperación de desastres del área de Informática y Tecnología, para el sistema Core del Negocio.

Riesgo 3: Modificación directa a la base de datos

Controles internos:	formulario "Solicitud de Petición Requerimiento para la Ejecución en la Base de Datos"
Pruebas de cumplimiento:	Existe el manual de "Gestión de Desarrollo de Software" no describe el procedimiento para modificaciones directas a las bases de datos que incluya los responsables de la autorización, así como la utilización del anexo 13 denominado "Solicitud de

	Petición Requerimiento para la Ejecución en la Base de Datos".
Pruebas sustantivas:	El área de tecnología realiza las afectaciones directas a las bases. Posee un formulario "Solicitud de Petición Requerimiento para la Ejecución en la Base de Datos" el nombre del aplicativo y la base de datos afectada. Lo expuesto ocasiona que se acceda, modifique o elimine inapropiadamente la información sensible de la cooperativa, poniendo en riesgo la integridad, disponibilidad y confidencialidad de la misma.

Riesgo 4: Clasificación de la información

Controles internos:	Existe procedimiento de tratamiento de la información
Pruebas de cumplimiento:	Registros de cómo lleva la institución la información clasificada
Pruebas sustantivas:	Se evidencia que la cooperativa lleva formularios de requerimientos autorizados para evidenciar que documentos son sensibles, confidenciales y públicos

Riesgo 5: Adquirir y Mantener Infraestructura Tecnológica

Controles internos:	Manual de adquisiciones institucional
Pruebas de	Durante la evaluación se observó que en la Cooperativa tiene

cumplimiento:	implementado como buena práctica de adquisición de infraestructura tecnológica, el reportar a la gerencia a través de la entrega de un informe en cual se explica el proceso de licitación, evaluación y adjudicación de tres proveedores, manteniendo una línea base común de requerimientos hacia dichos proveedores.
Pruebas sustantivas:	El desarrollo de un Plan de Adquisición de Infraestructura Tecnológica es importante ya que los cambios a la infraestructura para cada nueva aplicación se realizaran en conjunto con el negocio, dando un norte hacia los requerimientos futuros de escalabilidad, riesgos y vida útil de la inversión para actualizaciones de tecnología.

Riesgo 6: Claves de acceso a sitios Web

Controles internos:	Las funciones las realizan personas de diferentes Departamentos.
Pruebas de cumplimiento:	Tienen segregado funciones, para la entrega de sobres, emisión de claves.
Pruebas sustantivas:	De la revisión a la emisión de claves para este canal se pudo evidenciar que no existen niveles adecuados de seguridad respecto a la confidencialidad de las claves entregadas a los clientes. Es así que el usuario y la clave de la web son fácilmente visibles en los sobres donde se encuentran impresos. El uso indebido y manipulación de la información,

	podría instrumentarse en un posible fraude interno, en consecuencia tendría la institución pérdida económica y de imagen

Riesgo 7: Desempeño y Capacidad del Hardware

Controles internos:	Procedimientos vigentes
Pruebas de cumplimiento:	Durante la revisión se identificó que se encuentra el servidor de producción de la Cooperativa, respecto al core bancario, con la expectativa de la mejor utilización de sus recursos tecnológicos que redundarán en un mejor servicio para los usuarios internos así como para los clientes.
Pruebas sustantivas:	En la evaluación al ambiente de infraestructura se revisó los siguientes puntos: Configuración de permisos de acceso de comunicaciones Configuración del motor transaccional Conexión con base de datos Variables de entorno del sistema Al no llevarse una adecuada gestión de los datos de auditoría y transacciones de servicio se corre el riesgo de ocupar espacio innecesario utilizando recursos de máquina y almacenamiento.

Riesgo 8: Monitoreo d Base de Datos Transaccional

Controles internos:	Se realiza una revisión completa de todas las bases para obtener estadísticas del tiempo de ejecución con lo cual podrán calendarizar adecuadamente la realización de esta tarea
Pruebas de cumplimiento:	El procedimiento empleado para llevar a cabo esta tarea, especialmente para evitar la suspensión del servicio de base de datos durante la misma, era la de restaurar respaldos de las bases del Servidor de Producción sobre el equipo de desarrollo, lugar en donde se realizaba la revisión de consistencia. No se ha estado llevando un registro de novedades encontradas durante la revisión de la consistencia.
Pruebas sustantivas:	Se evidenció que con una mejora en el procedimiento de revisión de consistencia fue implementada la opción de checkstorage desde hace dos semanas atrás. Se han realizado pruebas de revisión dos bases grandes obteniéndose mejoras considerables en el tiempo de ejecución. Se nos comentó también que se realizara una revisión completa de todas las bases para obtener estadísticas del tiempo de ejecución con lo cual podrán calendarizar adecuadamente la realización de esta tarea

Riesgo 9: Monitoreo de las Redes LAN, WAN

Controles internos:	Implementación de herramientas informáticas en software y hardware de monitoreo.
Pruebas de	Registros de la implementación, descripción de lo implementado,

cumplimiento:	con los responsables
Pruebas sustantivas:	Testing de la aplicación de la metodología de segmentación de las redes, revisando los log de los equipos y evidenciando si no existe vulnerabilidades

Riesgo 10: Proveedores de Hardware

Controles internos:	El registro de sucesos de errores presentados en el servidor nos servirá En caso de que se presente algún error, este se registre en un documento formal de los problemas reportados y las soluciones empleadas. Adicionalmente nos servirá para tener una base centralizada de conocimiento.
Pruebas de cumplimiento:	Se evidenció que se mantiene un registro de sucesos de la base de datos en el caso de una bajada de servidor nos permitirá ver si fue por una bajada planeada o si se debió a algún problema. En el caso de que el motivo haya sido por algún problema, se podrá ver el detalle del mismo, la solución planteada y la posible manera de evitarlo. Si en algún momento en el futuro se presenta nuevamente el problema, se sabrá dar una solución de manera más rápida.
Pruebas sustantivas:	En la evaluación se evidencio que no se tiene proveedores alternos en caso de que fallen los sistemas de misión crítica, provocando una paralización del negocio en caso de que surja un evento de riesgo.

Riesgo 11: Respaldos de configuración

Controles internos:	El servidor de borde con sistema operativo GNU/Linux CentOS 5.4 modificado (NetCyclon de Hightelecom) en su interfaz de administración posee un sistema de respaldo de configuraciones
Pruebas de cumplimiento:	Es indispensable programar en el servidor tareas de respaldos de configuraciones de los archivos principales de servidos configurados. Para ello hay que realizar un cronogramas de cambios de configuraciones y en base a este cronograma proceder a realizar el respaldo de configuraciones
Pruebas sustantivas:	Se evidenció que el servidor de borde consta con la Base de Datos MySql y por motivo de configuraciones de esta aplicación de la empresa High se consideró no explorar sus configuraciones ya que al hacerlo podría causar alguna falla de grande dimensiones en la configuración del servidor. Del mismo modo se debe considerar la ejecución de: Respaldos completos Respaldos incrementales Respaldos diferenciales Con el objetivo de disminuir este riesgo mencionado. Principales de servidos configurados. Para ello hay que realizar un cronogramas de cambios de configuraciones y en base a este cronograma proceder a realizar el respaldo de configuraciones

3.1.2.6 Actividades de control

a. Controles existentes

Objetivo de control: Planificación y Control

Riesgo 1

Riesgo:	Uso de claves compartidas
Control:	Manual de Planificación y Control de IT

Riesgo 2

Riesgo:	Destrucción de información mal intencionada
Control	Tecnológicamente están establecidas seguridades, el riesgo se trasfiere al operativo (conozca a su empleado)

Riesgos 3

Riesgo:	Concentración de funciones
Control:	Se ha distribuido de una mejor manera para balancear las responsabilidades

Riesgo 4

Riesgo:	Códigos de acceso de personas desvinculadas se mantiene activo
Control:	Existe una buena práctica de ejecución en los sistemas

Riesgos 6

Riesgo:	Política de Seguridad de la información se encuentra desactualizada y no ha sido socializada
Control:	Moderado

Objetivo: Explotación y Soporte del TI

Riesgos 1

Riesgo:	El acceso al Data Center tiene seguridades físicas limitadas
Control:	Se han implementado seguridades físicas de mitigación de incendio, más sensible

Riesgo 2

Riesgo:	No se cuenta con procedimientos estandarizados del control de cambios a nivel de hardware y software
Control:	Manual de Gestión y Explotación de TI

Riesgo 3

Riesgo:	No se cuenta con herramientas de monitoreo de las comunicaciones
Control:	Implementación de equipo de monitoreo (What up)

Riesgo 4

Riesgo:	No se cuenta con una red LAN no segmentada (plana)
Control:	Implementación de metodología de segmentación por Vlan y agrupamiento

Riesgo 5

Riesgo:	Data Center limitado en espacio físico y distribución
Control:	Alto

Riesgo 6

Riesgo:	Sitio alterno con mínimas adecuaciones lógicas y físicas
Control:	Presupuesto para adecuaciones

Riesgo 7

Riesgo	El personal tiene escasa capacitación especializada en eventos externos
Control:	Proceso de capacitación en mitigación de incendios

Riesgo 8

Riesgo:	Monopolio de la empresa de soporte y mantenimiento
Control:	Se ha diversificado a los proveedores en su mayoría

En base a la matriz de riegos tecnológicos identificados, se detallan a continuación las pruebas de cumplimiento y sustantivas de los riesgos con mayor riesgo residual.

Tabla 24: Matriz de controles a riesgos tecnológicos

Subproceso	Responsable del Proceso	Descripción del Riesgo	Control	Efectividad del Control Impacto	Efectividad del Control Probabilidad	Riesgo Residual
PLANIFICACIÓN Y CONTROL	Tecnología	Uso de claves compartidas	Manual de Planificación y Control de IT	Muy bajo	Medio	Moderado
	Jefe de Informática y Tecnología	Instalación de software no autorizado	implementación de politicas y directrices en equipo Fortinet y Active directory	Muy alto	Muy alto	Bajo
	Jefe de Informática y Tecnología	Destrucción de información mal intencionada	Tecnologicamente están establecidadas seguridades, el riesgo se trasfiere al operativo (conozca a su empleado)	Medio	Bajo	Moderado
	Jefe de Informática y Tecnología	Modificación no autorizada de software	Procedimiento de implementación de software (Manual de Gestión y desarrollo), pruebas, bitacoras	Medio	Medio	Bajo
	Jefe de Informática y Tecnología	Concentración de funciones	Se ha distribuido de una mejor manera para balancear las responsabilidades	Muy bajo	Muy bajo	Moderado
	Jefe de Informática y Tecnología	Robo de software institucional	Programación del Copy Right en el software, al personal se hizo firmar un contrato de confidencialidad	Medio	Muy bajo	Bajo
	Tecnología	UC, OLA, con proveedores	los proveedores se hace firmar dichos	Muy bajo	Muy bajo	Bajo
	Jefe de Informática y Tecnología	Los programas desarrollados por la institución no se encuentran registrados en el Instituto Ecuatoriano de la Propiedad	Programación del Copy Right en el software, al personal se hizo firmar un contrato de confidencialidad	Medio	Muy bajo	Bajo
	Jefe de Informática y Tecnología	Deterioro de los respaldos de información	Manual de Planificación y Control de IT	Alto	Muy bajo	Bajo
	Jefe de Informática y Tecnología	Abuso de información privilegiada	información, tecnologicamente se maneja formulario de requerimientos	Muy bajo	Alto	Moderado
	Jefe de Informática y Tecnología	Instalación de hardware no autorizado en los equipos de	Manual de Gestión y Explotación de TI	Muy bajo	Bajo	Bajo
	Tecnología	Sustracción de hardware	se debe difundir y socializar al personal	Bajo	Medio	Bajo
	Jefe de Informática y Tecnología	encuentran los backups de los equipos de computo son	Manual de Gestión y Explotación de TI	Medio	Muy bajo	Bajo
	Jefe de Informática y Tecnología	Códigos de acceso de personas desvinculadas se mantiene activo	Existe una buena practica de ejecución en los sistemas	Muy bajo	Muy bajo	Moderado
	Jefe de Informática y Tecnología	No se lleva un registro de las personas que acceden a áreas	Existe las bitacoras de accesos al centro de computo.	Medio	Muy bajo	Bajo
	Jefe de Informática y Tecnología	El centro de computo no reúne condiciones físicas idóneas para mitigación de eventos externos tales como: incendios,	Se han implementado seguridades físicas de mitigación de incendio, más sencibles	Alto	Muy bajo	Bajo
	Jefe de Informática y Tecnología	No se cuenta con personal entrenado para enfrentar eventos	El personal esta basicamente entrenado para eventualidades de incendio	Medio	Muy bajo	Bajo
	Jefe de Informática y Tecnología	Politica de Seguridad de la información se encuentra desactualizada y no ha sido	Se han realizado capacitaciones y talleres para la socialización	Muy bajo	Muy bajo	Moderado

EXPLOTACIÓN Y SOPORTE IT	Administrador Centro de computo	El acceso al Data Center tiene seguridades físicas limitadas	Se han implementado seguridades fisicas de mitigación de incendio, más sencibles	Muy bajo	Muy bajo	Moderado
	Administrador Centro de computo	No se cuenta con procedimientos estandarizados del control de cambios a nivel de hardware y	Manual de Gestión y Explotación de TI	Alto	Muy bajo	Moderado
	Administrador Centro de computo	No se cuenta con herramientas de monitoreo de las comunicaciones	Implementación de equipo de monitoreo (What up)	Muy bajo	Muy bajo	Moderado
	Administrador Centro de computo	No se cuenta con una red LAN no segmentada (plana)	implementación de metodología de segmentación por Vlan y agrupamiento	Muy bajo	Muy bajo	Alto
	Administrador Centro de computo	Data Center limitado en espacio físico y distribución	Se ha realizado una redistribución de los equipos	Muy bajo	Muy bajo	Alto
	Administrador Centro de computo	Sitio alterno con minimas adecuaciones lógicas y físicas	Presupuesto para adecuaciones	Alto	Muy bajo	Moderado
	Administrador Centro de computo	El personal tiene escasa capacitación especializada en	Proceso de capacitación en mitigación de incendios	Muy bajo	Muy bajo	Moderado
	Administrador Centro de computo	Monopolio de la empresa de soporte y mantenimiento	Se ha diversificado a los proveedores en su mayoria	Bajo	Muy bajo	Moderado
	Administrador Centro de computo	Ataques externos a las redes	Se realiza pruebas de Ethicl Hacking y se implementó un equipo de seguridad para bloqueo de accesos externos	Bajo	Medio	Moderado
	Administrador Centro de computo	Manipulación de la configuración de Equipos	Implementacion de mejores y nuevas politicas de restricción a los accesos mediante herramientas de Active directory	Medio	Medio	Bajo
	Administrador Centro de computo	Denegación del servicio de red	Manual de Planificación y Control de IT	Muy bajo	Medio	Moderado
	Administrador Centro de computo	Personal clave no disponible	segregación de funciones y existencia de backup	Bajo	Bajo	Bajo

GESTIÓN Y DESARROLLO DE SOFTWARE	Administrador de TI	proyectos informáticos sin	Gerencia General	Bajo	Medio	Bajo
	Administrador de TI	Cambios de requerimientos que precisan modificaciones en la	Manual de Gestion y Desarrollo de software (procedimiento de cambios al software)	Medio	Muy bajo	Bajo
	Administrador de TI	Errores de mantenimiento / actualización de programas	Manual de Gestion y Desarrollo de software (procedimiento de paso a producción, proc de actualización o cambio de software, proc de actualizacion de programas COBIS)	Medio	Muy bajo	Bajo
	Administrador de TI	Utilización de Software ilegal	Implementación de controles como active directory y perfiles de acceso como politicas	Alto	Bajo	Bajo
	Administrador de TI	Modificaciones no autorizadas de datos	Tiene perfiles de autorización a la BDD, activada la auditoria a la BDD, existe procedimiento cambio y afectación a los datos	Medio	Medio	Bajo
	Administrador de TI	No se cuenta con una clasificación de la información de acuerdo a su grado de	Tiene perfiles de usuario a nivel de dominio, permisos transaccionales en el core bancario	Medio	Medio	Bajo
	Administrador de TI	Suplantación de la identidad del usuario	Envio de clave al corre y entrega de clave al usuario del servicio.	Medio	Medio	Bajo
	Administrador de TI	Fuga de información privilegiada	Perfiles de usuario, actualización de politicas y directrices del antivirus	Medio	Bajo	Bajo
	Administrador de TI	El tiempo requerido para desarrollar el proceso de	Basada en la metodología de puntos de fusión y casos de uso, además por jucio de	Medio	Medio	Bajo

Políticas y Procedimientos

Un factor primordial para el control de las operaciones financieras y los riesgos, exige el involucramiento de todas las unidades de la cooperativa, así como también el directorio, funcionarios y empleados.

En la evaluación efectuada, se evidencia que los eventos de riesgo más vulnerables son los factores de riesgo externos, en el proceso de lavado de activos, que la institución tiene políticas y procedimientos que por normativa lo aplicado la institución.

La institución ha empezado a estructurar un marco de gestión de riesgo operacional, a más de aplicar políticas y procedimientos a los riesgos más relevantes, este marco apunta a tres directrices: Cultural, Gestión cualitativa y Gestión cuantitativa.

Tabla 25: Gestión cuatitativa y gestión cualitativa

CULTURA	**GESTIÓN CUALITATIVA**	**GESTIÓN CUANTITATIVA**
Concientización sobre la importancia del riesgo operativo de la institución	Definición de la estructura organizativa y políticas, procesos, procedimientos	Captura de Datos y mantenimiento
	Identificación de riesgos, mapa de riesgos y respuesta, base de datos	Desarrollo de modelos de cuantificación, BIA, modelos probabilísticos,

	de eventos.	de perdidas esperadas,
	Desarrollo de indicadores y auto-evaluación	Calculo de capital con modelos estadísticos
		Integración de gestiones cualitativas y cuantitativas

Fuente: COAC Alianza del Valle

Con la implementación del software de gestión de riesgo “ERA”, se han realizado mejoras a las políticas y procedimientos dándoles un enfoque de riesgos. Para facilitar su prioridad, los planes de acción definidos para “atacar” las causas de pérdidas operacionales se han acompañado de un análisis costo/beneficio de su implementación

Para lograr los objetivos institucionales y los resultados planteados, las organizaciones requieren gestionar sus actividades y recursos con la finalidad de orientarlos hacia la consecuencia de metas, lo que se ha evidenciado la necesidad de adoptar herramientas y metodologías que permitan a las instituciones conocer a profundidad las actividades que llevan a cabo.

La intención de la cooperativa, es demostrar la capacidad para proporcionar servicios que contribuyan a la satisfacción del cliente interno y externo, a través de la aplicación eficaz de las políticas, procedimientos, indicadores y procesos de mejora continua, que aportan a la cooperativa a elaborar metodologías, responsabilidades, recursos, para ser evaluadas las actividades se están

ejecutando, lo cual permitirá identificar donde se encuentran las necesidades de mejora.

El Área de Gestión de Calidad evalúa el cumplimiento de las políticas y procedimientos de la institución, así como informa el incumplimiento de los mismos para la ejecución de los correctivos y mejoras continuas, cumpliendo la metodología del círculo de Deming.

3.1.2.7 Información y comunicación

La difusión que se hace es una reunión entre el auditado y el auditor y se lee el borrador del informe se discute y luego envían el informe final, luego la Gerencia General da a conocer a los involucrados el cumplimiento elaborándose cronogramas de seguimiento en unas matrices.

3.1.3 Fase III: Informe

La cooperativa en auditorias anteriores evidencia la existencia de una lectura preliminar de borrador con los dueños de los procesos auditados y al final se emite el informe definitivo a la gerencia general y este a su vez realiza la entrega del documento al responsable de la auditoria interna de la cooperativa para que se proceda a dar el seguimiento correspondiente.

Para este trabajo, en el informe de la auditoría realizada se hacen constar las los respectivos hallazgos para cada componente de COSO ERM así como las debidas recomendaciones que se detallen en el CAPÍTULO IV.

3.1.4 Modelo de madurez de los 8 componentes de coso ERM aplicados en la auditoría

Para emitir una opinión sobre la base de lo auditado contemplando los ocho componentes de COSO ERM nos basaremos en el enfoque del modelo de madurez para el control sobre los proceso de riesgo operativo que consiste en desarrollar un método de asignación de puntos para calificar a la institución desde inexistente hasta optimizada (de 0 a 5). Este planteamiento se basa en el Modelo de Madurez que el Software Engineering Institute definió para la madurez de la capacidad de desarrollo de software. (Ontoria Gonzalo, 2011)

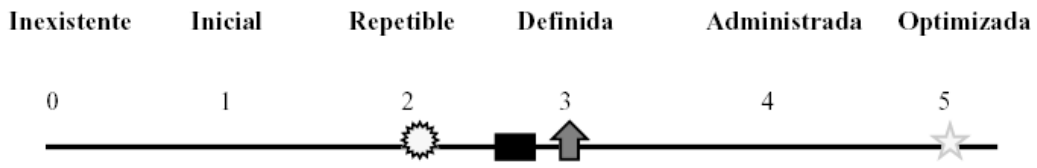
Los niveles de madurez basándose en los 8 componentes de COSO ERM del examen realizado a la cooperativa con marco de referencia COSO ERM se reflejan en la siguiente tabla:

Tabla 26: Modelo de madurez

RESUMEN GERENCIAL DEL MODELO DE MADUREZ PARA LOS COMPONENTES DE COSO ERM EN LA AUDITORIAS

	Componente COSO ERM	Descripción	Inexistente	Inicial/Ad Hoc	Repetible pero	Proceso definido	Administrable y medible	Optimizado
			0	1	2	3	4	5
1	**Ambiente Interno**	Filosofia de la gestion de Riesgo, cultura de riesgo, consejo de admonistración / direccion, valores eticos compromiso, estructura organizacional politicas y practicas de recursos humanos						
2	**Establecimiento de Objetivos**	Objetivos estratégicos, objetivos relacionados, riesgos aceptados, tolerancia al riesgo						
3	**Identificacion de eventos**	Eventos, eventos interdependientes, catagoria de eventos, riesgos y oportunidades						
4	**Evaluacion de Riesgos**	Riesgos inherentes y residuales, probabilidad e impacto, fuentes de datos, evaluación						
5	**Respuesta al Riesgo**	Evaluación de posibles respuestas, selección de respuestas						
6	**Actividad de control**	Integración de la respuesta al riesgo, tipos de actividades de control, politicas y procedimientos, controles de TI.						
7	**Información y comunicación**	Información y comunicación						
8	**Supervisión (Monitoreo)**	Actividades permanentes de supervisión - comunicación de deficiencias						

Fuente: COAC Alianza del Valle



LEYENDA PARA LOS SÍMBOLOS USADOS	LEYENDA PARA LAS CLASIFICACIONES USADAS
Situación actual de la empresa Lineamientos Estándar Internacionales Mejor Práctica de la Industria Estrategia de la Empresa	0 Inexistente - los procesos de administración no se aplican en absoluto 1 Inicial - Los procesos son ad hoc y desorganizados 2 Repetible - Los procesos siguen un patrón regular 3 Definida - Los procesos son documentados y comunicados 4 Administrada - Los procesos son monitoreados y medidos 5 Optimizada - Las mejores prácticas son seguidas y automatizadas

Para cada uno de los 8 componentes de COSO ERM, utilizaremos una escala gradual ascendente de medidas, basada en una clasificación de “0” hasta “5”. La escala está asociada con las descripciones del modelo genérico cualitativo de madurez que van desde “Inexistente” hasta “Optimizada” de la forma siguiente:

MODELO GENÉRICO DE MADUREZ
0 Inexistente. Total falta de un proceso reconocible. La organización ni siquiera ha reconocido que hay un problema que resolver.
1 Inicial. Hay evidencia de que la organización ha reconocido que los problemas existen y que necesitan ser re sueltos. Sin embargo, no hay procesos estandarizados pero en cambio hay métodos ad hoc que tienden a ser aplicados en forma individual o caso por caso. El método general de la administración es desorganizado.
2 Repetible. Los procesos se han desarrollado hasta el punto en que diferentes personas siguen procedimientos similares emprendiendo la misma tarea. No hay capacitación o comunicación formal de procedimientos estándar y la responsabilidad se deja a la persona. Hay un alto grado de confianza en los conocimientos de las personas y por lo tanto es probable que haya errores.
3 Definida. Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones. Los procedimientos mismos no son sofisticados sino que son la

formalización de las prácticas existentes.
4 Administrada. Es posible monitorear y medir el cumplimiento de los procedimientos y emprender acción donde los procesos parecen no estar funcionando efectivamente. Los procesos están bajo constante Mejoramiento y proveen buena práctica. Se usan la automatización y las herramientas en una forma limitada o fragmentada.
5 Optimizada. Los procesos han sido refinados hasta un nivel de la mejor práctica, basados en los resultados de mejoramiento continuo y diseño de la madurez con otras organizaciones. TI se usa en una forma integrada para automatizar el flujo de trabajo, suministrando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte con rapidez.

Este enfoque de Modelo de Madurez permitirá a la administración de la cooperativa ponerse en la escala y apreciar lo que está involucrado si necesita mejorar el desempeño. La escala incluye 0 a 5 porque es bastante probable que no exista ningún proceso en absoluto. La escala 0-5 se basa en una escala simple de madurez que muestra cómo evoluciona un proceso desde Inexistente hasta optimizado. Debido a que son procesos de administración, la madurez y la capacidad aumentada es también sinónimo de mayor manejo del riesgo y mayor eficiencia.

El Modelo de Madurez es una forma de medir qué están bien desarrollados los procesos de administración.

CAPITULO IV

4.1 Informe auditoría Cooperativa Alianza del Valle

4.1.1. Antecedentes

La auditoría se la realizó en función de una planificación previamente establecida y aprobada por las autoridades institucionales, utilizando entrevistas, observación y obtención de información sostenida con el personal del Área de Auditoría Interna; Unidad de Riesgos; Tecnología de la Cooperativa de Ahorro y Crédito Alianza del Valle, donde se efectuó evaluaciones de ambiente interno, identificación de objetivos y riesgos, evaluación del riesgo, respuestas a los riesgos, controles de TI (Tecnología de Información) existentes principalmente.

Los comentarios y sugerencias que se exponen a continuación surgen de los procedimientos aplicados durante la revisión. La intención de las situaciones observadas tiene como finalidad ayudar en la toma de decisiones y en la optimización de controles de los recursos informáticos de la cooperativa.

Normativa aplicativa y excepciones

Las normativas aplicadas en el examen de auditoría son:

NORMAS GENERALES PARA LA APLICACIÓN DE LA LEY GENERAL DE INSTITUCIONES DEL SISTEMA FINANCIERO TITULO X.- DE LA GESTION Y ADMINISTRACION DE RIESGOS CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO (capítulo incluido con resolución No JB-2005-834 de 20 de octubre del 2005

COSO ERM Committee of Sponsoring Organizations of the Treadway Commission, enuncio um marco de control mejorado del COSO, denominado COSO –ERM, (Enterprise Risk Management), basado en el riesgo.

Resolución JB-2012-2148 de julio de 2012", Informe de Análisis GAP PCI DSS, de diciembre de 2011 y el Informe borrador de auditoría informática, de Diciembre de 2010.

Art. 5 de la sección III Administración del Riesgo Operativo, del capítulo V, título X De la Gestión y Administración de Riesgos.

Art.9 de la sección III, de la "Administración de Riesgos", del capítulo I, Título X de la Gestión de Riesgos, de la Codificación de Resoluciones de la SBS y JB.

4.1.2 Objetivos de la Auditoría Informática

✓ Determinar el cumplimiento y la substanciación los riesgos operativos tecnológicos enunciados en la norma JB 834 de de la Superintendencia de Bancos y Seguros como factor de la eficiencia y productividad de la COAC Alianza del Valle.

4.1.3 Alcance de la Auditoría Informática

La auditoría está orientada a examinar los riesgos tecnológicos más relevantes que enuncia la norma SBS - JB 834, realizando pruebas de cumplimiento y substanciación de los riesgos donde el impacto afecte la cadena de valor del negocio.

Las pruebas de cumplimiento se identificarán los controles clave que deben probarse, realizando pruebas de confiabilidad, prevención de riesgos y adherencia a las políticas y procedimientos de la organización.

En las pruebas de substanciación se aplicarán procedimientos detallados de análisis de datos donde los controles sean débiles y el impacto sea alto.

4.1.4 Hallazgos y Recomendaciones con enfoque en COSO ERM

La Auditoría presenta una dimensión de los resultados, un análisis de impacto general, oportunidades de mejora, conclusiones y recomendaciones.

4.1.4.1 Ambiente Interno

H1: El Código de Ética aplicará no se socializa a todos los directivos, funcionarios y empleados de la Cooperativa, lo expuesto conlleva a que no se dé cumplimiento a las políticas institucionales con respecto a los riesgos, así como los proyectos importantes de la organización que asegurar el logro de los objetivos corporativos.

R1: La Gerente General dispondrá que el Jefe de Talento Humano, que la asignación de funciones, deberes y responsabilidades se le comunique formalmente por escrito a cada empleado dejando constancia con las firmas de responsabilidad, la no comunicación formal existe el riesgo de incumplimiento de funciones.

H2: El Código de Ética está estructurado de tal manera que facilita el cumplimiento y la puesta en práctica del quehacer profesional con acento en la propuesta de criterios de acción y conducta, es necesario incluir el mensaje de los directivos, especialmente de la Gerencia General para lograr el empoderamiento institucional y la integridad ética para la Cooperativa.

R2: La Gerencia General dispondrá al Jefe de Gestión de Calidad que se incluya en el Código de Ética el mensaje de los directivos, especialmente de la Gerencia General para lograr el empoderamiento institucional y la integridad ética para la Cooperativa.

H3: La cooperativa no cuenta con un comité de sistemas con responsabilidades formalmente definidas que constituya un apoyo para la gestión del área de tecnología y mantenga reuniones periódicas, cuyas decisiones queden plasmadas en un acta. En la actualidad los temas de tecnología son revisados y aprobados por el comité integral de riesgos; en donde uno de sus miembros es el responsable del área tecnología con una participación exclusivamente de voz.

R3: La Gerencia General dispondrá la creación Comité de Tecnología que esté conformado por los representantes de las áreas más importantes de la cooperativa. Los miembros de dicho Comité deberán conocer y aprobar las políticas, procedimientos y las prácticas del área de tecnología, para ello deberán contar al menos Funciones y procedimientos formalmente definidos y aprobados por el Consejo de Administración.

4.1.4.2 Establecimiento de Objetivos

H1: Los objetivos de la organización buscan fortalecer la filosofía cooperativista, se establecen a corto, mediano y largo plazo. Los objetivos estratégicos constituyen la base para los objetivos operacionales.

R1: La Gerencia General dispondrá a Jefe de Riesgos que establezca con claridad cuantitativa el impacto de los riesgos en los objetivos y los recursos en la cadena de valor de la institución. lo expuesto, se corre el riesgo de no dimensionar de manera eficiente y ordenada el crecimiento del negocio haciendo ineficiente el cumplimiento objetivos organizacionales.

H2: La cooperativa ha establecido una matriz de identificación de objetivos institucionales y riesgos operativos, no se ha establecido cuantificadamente la tolerancia la riesgo se evidencia detalladamente la situación actual, observaciones y recomendaciones para cada uno de los riesgos operativos como son personas, procesos, tecnología y eventos externos, según lo establecido en las NORMAS GENERALES PARA LA APLICACIÓN DE LA LEY GENERAL DE INSTITUCIONES DEL SISTEMA FINANCIERO TITULO X.- DE LA GESTION Y ADMINISTRACION DE RIESGOS CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO (capítulo incluido con resolución No JB-2005-834 de 20 de octubre del 2005) y recomendaciones de auditorías previas.

R2: La Gerencia General dispondrá al Jefe de Riesgos realizar un cruce entre objetivos institucionales con el riesgo aceptado para determinar la

tolerancia y el apetito al riesgo que la institución tiene. El no tener una relación de objetivos y los riesgos aceptados en la administración de riesgo que permitan medir el impacto ocasionado, pone en riesgo los esfuerzos y acciones que realizan las áreas hacia los objetivos institucionales.

H3: El riesgo aceptado se expresa en términos cualitativos, calificando de Alto, Moderado, Bajo, dejando de por lado una valoración cuantitativa para que de esta forma se evidencie el costo de las pendidas que se producen cuando se da un evento negativo se materializa en los procesos críticos de la cadena de valor.

4.1.4.3 Identificación de Eventos

H1: La cooperativa identifica los eventos potenciales para los riesgos operativos y los evalúa con el impacto y probabilidad para determinar la forma como pueden afectar la rentabilidad del negocio. Para la identificación de eventos de riesgo la cooperativa parte de un enfoque de procos (macroproceso, subproceso, proceso y evento). En este proceso la cooperativa cuenta con buenas prácticas metodológicas, categorizando en función del giro del negocio. Además especifica en su matriz de inventario de procesos y luego en la identificación de procesos críticos hasta un nivel de actividades.

R1: La Gerencia General dispondrá al Jefe de Riesgos Implementar una metodología para la administración de riesgos tecnológicos, tal metodología y estructura deberá incorporar una evaluación regular de los riesgos relevantes

de información para lograr los objetivos de la institución, conformando una base para determinar cómo deberían ser administrados los riesgos a un nivel aceptable. Lo expuesto pone en riesgo a la institución ya que no permitiría tomar acciones correctivas a tiempo.

H2: Los riesgos son identificados en función de probabilidad alta, media y baja con impacto similar, en los mapas establecidos para la valoración se evidenció, que para los riesgos de impacto y probabilidad de alta no cuenta con programas y planes de mitigación. Esta situación, podría afectar al éxito del desarrollo de los proyectos de la institución que apalancan los objetivos estratégicos.

R2: La Gerencia General dispondrá al Jefe de riesgos elabore una metodología para identificar las debilidades y las amenazas para los recursos de información utilizados con el fin de lograr los objetivos de la Institución. El proceso debería proveer evaluaciones de riesgo tanto a nivel global como a niveles específicos de sistemas, para proyectos nuevos así como sobre una base recurrente, y con participación multidisciplinaria. Para desarrollar un programa de administración de riesgos tecnológicos se deberá tomar en cuenta lo siguiente: Escoger un enfoque para proceso del cálculo del riesgo, teniendo en cuenta:

- Determinación del criterio para la aceptación del riesgo

Identificación de los niveles tolerancia al riesgo.

4.1.4.4 Evaluación del Riesgo

H1: La cooperativa tiene identificado y evaluado los riesgos inherentes y residuales, probabilidad e impacto, en matrices de Evaluación del Riesgo, donde se evidencia factores de riesgo origen del riesgo, probabilidad de ocurrencia, los niveles de riesgo inherente, controles, riesgo residual, tipo de riesgo, lo que no se evidencia es un análisis cuantitativo de los riesgos. De igual manera no se evidencia una administración de riesgos en la organización en los niveles de metas y objetivos tal como lo expresa las NORMAS GENERALES PARA LA APLICACIÓN DE LA LEY GENERAL DE INSTITUCIONES DEL SISTEMA FINANCIERO TITULO X.- DE LA GESTION Y ADMINISTRACION DE RIESGOS CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO (capítulo incluido con resolución No JB-2005-834 de 20 de octubre del 2005) y recomendaciones de auditorías previas. Lo expuesto pone en riesgo a la institución ya que no permitiría tomar acciones correctivas a tiempo.

R1: La Gerencia General dispondrá al Jefe de riesgos la implementación de un esquema de administración de riesgos tecnológicos para la cooperativa, tal estructura debería incorporar una evaluación regular de los riesgos relevantes de información para lograr los objetivos de la institución, conformando una base para determinar cómo deberían ser administrados los riesgos a un nivel aceptable.

H2: La cooperativa no tiene buenas prácticas formalizadas de respuesta al riesgo, procede a priorizarlos bajo un enfoque de riesgo residual. Se evidencia

que en los riesgos residuales de calificación alta se elaboran planes y programas de acción, donde se refleja la aversión al riesgo (aceptar, compartir, reducir, evitar); luego de identificado los riesgos se procede a tomar las medidas tendientes a evitar que impidan el cumplimiento de los objetivos, tampoco ha establecido matrices para establecer la vinculación, en su defecto lo que ha elaborado es matrices de los procesos críticos.

R2: Se recomienda que la Gerencia General disponga al Comité integral de Riesgo la elaboración de matrices para evidenciar el riesgo aceptado de los procesos críticos que afectan a los procesos operativos

4.1.4.5 Actividades de Control

H1: La cooperativa ha establecido que luego de la “aversión al riesgo”, se establecen actividades específicas para el riesgo residual tomando acciones preventivas, detectivas, generando políticas, procedimientos, automatización de controles que están incorporadas en las operaciones del negocio, que se aplica a toda la cooperativa. Además para cada uno de los controles implementados se realizan las respectivas pruebas de cumplimiento y sustantivas están relacionadas con los principales riesgos tecnológicos.

R1: La Gerencia General dispondrá se formalice un estándar para respuestas al riesgo y los riesgos residuales identificados como altos a través de programas de mitigación. El no contar con una actividad de control y auditoría continua, y la generación de buenas prácticas pondría en riesgo a la

entidad en caso no valorar los procesos críticos y tener inversiones no sustentadas en la mitigación.

H2: Se evidencio que la Unidad de Riesgos recibe los informes del comité Integral de Riesgos (CAIR), donde están plasmados informes ejecutivos de los resultados obtenidos de los seguimientos realizados. Además el Jefe de Riesgos presenta información a los entes de control para el seguimiento respectivo. No existe evidencia clara que se comunique a toda la organización. La falta de comunicación y socialización pone en riesgo a la institución ya que no permitiría tomar acciones correctivas a tiempo en condiciones preventivas.

R2: Se recomienda que la Gerencia General disponga al Jefe de Riesgos conjuntamente con el Jefe de Tecnología actualicen la matriz de riesgos inherente y residuales, para identificar los riesgos con mayor riesgo residual y poder aplicar los controles necesarios donde el impacto no sea muy alto y el control sea eficiente

4.1.4.6 Información y Comunicación

H1: La cooperativa realiza seguimiento por medio del Jefe de Riesgos y del Auditor interno, pero no se hace una eficiente medición del control aplicado; se evidencia que se ha establecido una metodología Delphi o de juicio de expertos, para valorar o emitir juicios objetivos que al no tener una valoración sustentada existe el riesgo de decisiones que afecten a los objetivos de negocio de la institución.

R1: La Gerencia General dispondrá que el Jefe de Riesgos elabore e implementará una metodología o desarrollará sus propias técnicas o esquemas de administración, considerando su objeto social, tamaño, naturaleza, complejidad y demás características propias. Observar y cumplir con lo dispuesto en la sección III Administración del Riesgo Operativo en los temas pertinentes fortaleciendo la administración.

H2: Se evidencio la existencia y seguimiento de las recomendaciones establecidas por auditorías informáticas externas realizando matrices de seguimiento, donde establecen el tiempo, responsables y se realizan ajustes a las matrices de riesgo en función de los avances y/o nuevas observaciones que se van incluyendo.

R2: El Auditor Interno deberá dar cumplimiento a lo establecido en los numerales 9.2, 9.3, 9.8, de la sección 1, Capítulo II, "Normas para la calificación de los auditores internos de las entidades sujetas al control de la Superintendencia de Bancos y Seguros.", título XXI, de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, con el fin de ahondar y extender sus exámenes periódicos y permanentes enviados al organismo de control y/o al Consejo de Administración, en especial lo que se refiere hacia controles para comprobar la existencia y adecuado funcionamiento de sistemas de control interno que garanticen el logro de los objetivos de la institución; así mismo, que evalúe los

recursos informáticos y sistemas de información de la entidad para establecer si proporcionan a la administración reportes oportunos y suficientes que permitan tomar decisiones e identificar posibles exposiciones de riesgo; así como también realizar un seguimiento a las observaciones de auditoría interna anteriores para verificar que los funcionarios y la administración, hayan adoptado sus recomendaciones para superar deficiencias comunicadas.

4.1.5 Conclusiones y Recomendaciones

Conclusiones

- En el proceso de auditoría se evidenció que la Cooperativa no tiene establecido una buena práctica con estándares internacionales que sirvan de referente para administrar y gestionar los riesgos operativos y generar valor al negocio, como también tener medidos los riesgos inherentes a través de buenos controles, generando un ciclo Deming a los riesgos residuales.

- Al aplicar COSO ERM como metodología de Evaluación y Auditoria a los riesgos operativos en cooperativa se evidenció que la gestión de riesgos corporativos no constituye un proceso en serie donde cada componente afecta sólo al siguiente, sino un proceso multidireccional en que casi cualquier componente influye en otro. De esta manera al ejecutar la auditoría a la cooperativa se muestra una escasa relación directa entre los objetivos que la entidad desea lograr y los componentes de la gestión de riesgos corporativos y lo que le hace falta para lograr aquellos.

- Aunque la gestión de riesgos corporativos proporciona ventajas importantes, en la evaluación realizada se evidenció ciertas limitaciones al auditar con COSO ERM. Además de los factores comentados anteriormente, existen limitaciones que se derivan de hechos como que el juicio de valor emitido por las personas puede ser erróneo o provocar un sesgo durante la toma de decisiones sobre la respuesta al riesgo y el establecimiento de controles que no supere a lo que se desea. Estas limitaciones impiden que Consejo o la Dirección tengan seguridad absoluta de la consecución de los objetivos de la entidad.

- Los métodos sofisticados de cuantificación resultan clave para calcular el capital en riesgo, pero por sí solos no aportan suficiente valor a la entidad ni a sus negocios. Los beneficios derivados de la utilización de lo que se considera una metodología híbrida resultan más amplios, especialmente en aspectos relacionados con mejoras de procesos y para la generación de mejoras en eficiencia y efectividad. Cuando se habla de una metodología híbrida nos referimos a la utilización, no sólo de mediciones derivadas de distribuciones de pérdida, sino a la combinación de éstas con análisis de escenarios que requieren del juicio de los gestores de riesgo, así como también la inclusión de información interna de la entidad, además de informaciones obtenidas, de la elaboración de una base de datos de eventos.

- Para que la administración del riesgo operacional funcione resulta necesario que tenga bases concretas dentro de la estructura organizativa y de la alta dirección. Allí las buenas prácticas de gobierno corporativo y la

capacitación en temas de riesgo resultan ser fuertes mitigantes del riesgo, siempre que estén embebidas eficientemente dentro toda la organización. La responsabilidad por mantener el riesgo operacional siempre presente y por llevarlo a todos los niveles de la organización deberá recaer siempre en la alta gerencia y en la dirección de la entidad.

- Al realizar un examen de auditoría con marco de referencia COSO ERM es hacer una evaluación integral ya que audita empezando por la Dirección, Control interno, Riesgos importantes hasta llegar a los informes y monitoreo, cumpliéndose un circulo de mejora y genera valor para la institución esto como ventaja; la desventaja es un proceso muy extenso por sus ocho componentes y sus objetivos que involucra el marco.

Recomendaciones

- La Cooperativa debe elaborar, presentar e implementar planes de mitigación donde el riesgo residual es alto y permita mitigar la amenaza y permita avanzar y corregir en las dificultades que retrasan la operatividad de los diferentes procedimientos en estas Áreas involucradas en la cadena de valor y cumplir con los objetivos y políticas de calidad.
- Instruir y sensibilizar al personal encargado de los diferentes procesos que impactan en el giro del negocio, sobre la importancia de las matrices de riesgo, la Implementación de los indicadores de gestión, a efecto de minimizar los riesgos que puedan afectar el desarrollo de los procedimientos y poder cumplir con los planes estratégicos y operativos de la cooperativa.

- Las matrices de riesgo operativo, los indicadores de gestión y los controles de las Áreas, procesos o dependencias auditados, deben ser cuantificables a más de ser cualificables, aplicando lo que expone Basilea II en sus diferentes métodos de cálculo, permitiendo de esta manera tener el coste de una perdida.
- Se hace necesario fortalecer los controles en todos los procesos y procedimientos operativos minimice el riesgo residual y la pérdida esperada sea baja.
- La gestión de riesgos corporativos no constituye estrictamente un proceso en serie, donde cada componente afecta sólo al siguiente, sino un proceso multidireccional e iterativo en que casi cualquier componente puede influir en otro, por lo tanto la institución debe gestionar sus riesgos en función de sus procesos críticos que pueden afectar al giro del negocio.
- El software “ERA” que tiene implementado la institución al estar construido bajo las características de COSO ERM, es una herramienta informática que apoyaría en tener información más dinámicamente y tener una base de conocimiento para gestar los riesgos.

4.1.6 Opinión

4.1.6.1 Dictamen del auditor a la gerencia general

Se auditado el cumplimiento y sustanciación a la gestión de riesgos operativos con marco de referencia COSO ERM al cumplimiento y la

sustanciación de la resolución No JB-2005-834 de 20 de octubre del 2005 de la Cooperativa de Ahorro y Crédito Alianza del Valle, al 31 de julio del 2013, con mayor énfasis en los riesgos tecnológicos. La administración de los Riesgos es responsabilidad de la administración de la Cooperativa y la gestión del Comité y responsable de Riesgos. Mi responsabilidad es expresar una opinión sobre la situación actual al corte; de la administración y gestión de riesgos operativos basados en el examen de auditoría. Además cumplimiento de la Resolución 834 de la Superintendencia de Bancos y Seguros.

La auditoría fue realizada de acuerdo con el marco de referencia COSO ERM aplicable a la auditoría de los riesgos operativos. Dicho marco de referencia requiere que una auditoría sea planificada y ejecutada en base a 8 componentes en la administración y gestión de riesgos operativos de la institución para obtener un nivel de madurez aceptable. La auditoría incluye el examen, a base de pruebas de sustanciación sobre riesgos relevantes que afectan a la cadena de valor del negocio. Considero que la auditoría provee una base razonable para expresar una opinión.

En mi opinión:

a) El nivel de madurez es aceptable según la evaluación realiza que va desde 2 (repetible) donde sus procesos siguen un patrón y se proyectan a un nivel 4 (administrada) que visiona alcanzar que sus procesos sean monitoreados y medidos regularmente. Considerando que debe existir la mejora continua para que el nivel de exposición a los riesgos sea cada vez menor, aplicando programas de mitigación.

b) La Cooperativa es respetuosa en el cumplimiento de las regulaciones emitidas por los entes de control en resoluciones emitidas para la administración y gestión de riesgos operativos, respecto de todo lo importante.

El AUDITOR

4.1.7 Cierre

4.1.7.1 Contactos

Para cualquier tipo de inquietud, comentario, aclaración, requerimiento o demás, solicitamos comunicarse con el auditor:

Firma de Responsabilidad

Este documento se considera un documento formal y de muestra la responsabilidad de su autor.

CAPÍTULO V

5.1 Conclusiones y Recomendaciones

La investigación de campo y con los datos recopilados y analizados, se proporcionan las conclusiones respectivas, referentes a la elaboración de una Auditoría informática a los riesgos operativos. Con la finalidad de aportar elementos y herramientas valiosas para que el auditor desarrolle su trabajo de acuerdo al avance tecnológico. También se desarrollan las recomendaciones originadas del desarrollo del trabajo y el análisis de la investigación.

5.1.1 Conclusiones

A través de los resultados obtenidos en el presente trabajo, se determinó que la auditoría realizada demuestra el cumplimiento de los objetivos planteados, evidenciado los riesgos más relevantes, expuestos en matrices y mapas de calor.

COSO ERM, un marco de referencia de control interno que hace énfasis en sus 8 componentes y sus objetivos permiten hacer un análisis profundo y de agregar valor si se implementa como metodología.

5.1.2 Recomendaciones

- Según Basilea II expone que las instituciones cuantifiquen el riesgo provisionando contablemente y se cuantifique el riesgo utilizando diferentes métodos como del indicador básico, estándar y edición avanza.

- Con el avance de la tecnología se han dado modernos factores de riesgos operativos como:

- Procesamientos manuales se han potencializado y globalizados por el uso generalizado de tecnología.
- Crecimiento del e-commerce
- Surgimiento de nuevas instituciones financieras que tienen servicios complementarios
- Formas de mitigación del riesgo
- Masificación de las tercerizaciones y outsourcing

- La cooperativa debe generar un proceso para evaluar su suficiencia de capital en relación a su perfil de riesgo y una estrategia para mantener el nivel de capital.

- Se recomienda que reserve capital económico para protección contra pérdidas potenciales inherentes a las actividades del negocio,

- La auditoría informática es su estructura es compleja más aun cuando está enfocada en riesgos, por la recolección de evidencia para su evaluación de la información se recomienda mejorar la metodología planteada a partir de este modelo.

- Se recomienda realizar auditorías informáticas aplicando otros estándares y marcos referenciales enfocados en riesgos.
- Los hallazgos que se mencionan en la tesis considerarlos como fuentes didácticas académicas que pretenden exponer una metodología de examen de auditoría.

BIBLIOGRAFÍA

Coso. (09 de 2004). Recuperado el 28 de 01 de 2013, de http://www.coso.org/documents/coso_erm_executivesummary.pdf

Sistema Bibliotecario Matias. (2004). Recuperado el 21 de 01 de 2013, de http://webquery.ujmd.edu.sv/siab/bvirtual/Fulltext/ADCN0000558/Capitulo%201.pdf

(2011). *Agenda Política Económica del Buen Vivir.* Quito: Ministerio de la Coordinación de la Política Económica.

Dirección y Coordinación Técnica de Planificación. (06 de 2011). Recuperado el 28 de 01 de 2013, de http://www.fifomi.gob.mx/web/images/fifomi/documentos/normateca/mejorada/riegos/ma-dctyp-02.pdf

(2011). *Memoria COAC Alianza del Valle 2011.* Quito.

(2012). *Memoria COAC Alianza del Valle 2012.* Quito.

Net Consul.com. (2012). Recuperado el 28 de 01 de 2013, de http://www.netconsul.com/riesgos/cci.pdf

Registro Oficial No. 1061. (16 de 02 de 2012). *Reglamento a Ley Orgánica de Economía Popular y Solidaria*. Quito, Pichincha, Ecuador: Superintendencia de Economía Popular y Solidaria.

Universidad de la República de Uruguay, Control Interno. (12 de 10 de 2012). Recuperado el 29 de 01 de 2013, de http://ww.ccee.edu.uy/ensenian/catcoint/material/control.PDF

Alfaro, N. (2008). *Universidad Autónoma Tomás Frias.* Recuperado el 28 de 01 de 2013, de ://www.uatf.edu.bo/web_descargas/manual_aud_interna.pdf

Báez, B. (2010). *Matriz de Riesgo Operacional.* Paraguay: DGRV.

Brito, J. (2009). Recuperado el 05 de 01 de 2013, de Escuela Politectica del litoral: http://www.dspace.espol.edu.ec/bitstream/123456789/5667/2/Tesis.doc

COSO. (2004). *Informe Coso.*

Ferreas Salegre, A. (octubre de 2005). Riesgo Operativo en España.

García, J. (6 de septiembre de 2010). *Pérdida de Riesgo Operacional*. Recuperado el 07 de 01 de 2013, de

http://www.sbs.gob.pe/repositorioaps/0/0/jer/pres_doc_basilea/Bases_Datos_Eventos_Perdida_Riesgos_Operacionales%20.pdf

López, F. (2005). *La Gestión de riesgos en las Cooperativas de Ahorro y Crédito.* Recuperado el 21 de 01 de 2013, de http://www.aciamericas.coop/IMG/pdf/El_Riesgo_en_la_Gestin_Cooperativa.pdf

MIES. (2010-2013). *Agenda de la Revolución de la Economía Popular y Solidaria 2010-2013.*

Monografias.com. (s.f.). Recuperado el 27 de 01 de 2013, de http://www.monografias.com/trabajos12/coso/coso2.shtml

Ontoria Gonzalo, S. (2011). *Gobierno y Modelado de la Seguridad de la Información en las Organizaciones.* Madrid : Escuela Politécnica de Madrid.

Revista Seguridad. (2009). *Revista Seguridad*. Recuperado el 12 de 01 de 2013, de Resvista Seguridad: http://revista.seguridad.unam.mx/numero-14/riesgo-tecnol%C3%B3gico-y-su-impacto-para-las-organizaciones-parte-i]

Salnave, A., & Riaño, L. M. (2008). *Manual de Implementación.* Recuperado el 27 de 01 de 2013, de http://portal.dafp.gov.co/form/formularios