ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"Creación de un Marco de Control para la Administración del Riesgo Operativo relacionado con la Tecnología de Información como modelo para las Cooperativas de Ahorro y Crédito del Ecuador"

TESIS DE GRADO

Previa a la obtención del Título de:

MAGISTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

Presentado por:

Jimmy Arturo Brito Domínguez

Guayaquil-Ecuador

2009

AGRADECIMIENTO

A Jehová por todas sus bendiciones, su ayuda, protección y dirección durante toda mi vida.

A mis padres por darme su apoyo, amor y fortaleza en todo momento.

A mi esposa y mis hijos por darme todo su apoyo, comprensión y motivación para seguir adelante con este sueño.

Al Dr. Jorge Jácome por su apoyo, motivación y consejos.

Al Ing. Fabricio Echeverría y al Ing. Lenin Freire por su apoyo, dirección y guía para la realización de esta Tesis.

Al Ing. Jorge Olaya y la Ing. Karina Astudillo por sus recomendaciones y consejos para el mejoramiento de esta Tesis.

DEDICATORIA

A mi Mamá y mi Papá por su ejemplo y apoyo incondicional en todo momento.

A mi esposa y mis hijos.

A mis hermanos y toda mi familia.

A mis amigas y amigos.

TRIBUNAL DE GRADUACIÓN

Ing. Lenin Freire Cobo
DIRECTOR MSIG

Ing. Fabricio Echeverría
DIRECTOR DE TESIS

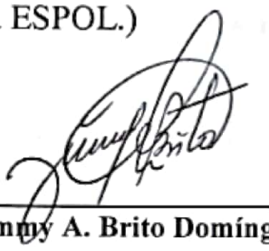
Ing. Jorge Olaya
MIEMBRO TRIBUNAL

Ing. Karina Astudillo
MIEMBRO TRIBUNAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITECNICA DEL LITORAL".

(Reglamento de Graduación de la ESPOL.)



Jimmy A. Brito Domínguez

RESUMEN

El crecimiento acelerado que han tenido las Cooperativas de Ahorro y Crédito en el Ecuador las ha convertido en instituciones financieras muy respetables y de amplia aceptación para muchos ciudadanos, quienes acuden a ellas en busca de un servicio de ahorro para sus recursos financieros y en la oportunidad de poder acceder a un crédito en forma oportuna y eficaz. Dicho crecimiento operacional y financiero ha significado también una expansión en su cobertura, productos y servicios en forma muy similar a la de los bancos mediante el uso de la tecnología y los sistemas de información.

Dicho uso creciente de la tecnología de información por parte de las COAC's conlleva también una mayor dependencia hacia ella y por lo tanto, los riesgos relacionados a la tecnología de información se transfieren a los procesos del negocio; lo cual, involucra una responsabilidad para la Alta Dirección respecto a la administración de los riesgos relacionados con la tecnología de información ya que el no hacerlo podría poner en riesgo la seguridad de uno de sus activos más importantes: la información; y, la continuidad de sus operaciones, acarreando incuantificables pérdidas financieras y hasta la desaparición de la Entidad.

Es por ello, que tanto organizaciones internacionales como gubernamentales de nuestro País han emitido una serie de normas, estándares y mejores prácticas como: COSO-ERM, COBIT, ITIL, ISO 27001 y la Resolución denominada 834, que permitan a las Entidades Financieras y muy en particular a las COAC's, poder hacer frente al desafío de lograr una adecuada administración de los procesos, las personas, la tecnología y los eventos externos en forma efectiva y sustentable, bajo un adecuado ambiente de control interno.

Por consiguiente, para el éxito dentro de la administración del riesgo tecnológico es necesario el liderazgo de la Alta Dirección y el compromiso de todos quienes conforman la Entidad hacia una cultura de control interno y prevención del riesgo, basado en los diferentes lineamientos, marcos de referencia, estándares y regulaciones vigentes, adaptado a las necesidades y requerimientos de cada Entidad, buscando la seguridad de la información y la continuidad del negocio en

forma sustentable; de tal manera, que se agregue valor y ventaja competitiva a las operaciones que realizan.

Es necesario que las COAC's diseñen, implementen y mejoren una metodología para la administración del riesgo operativo, considerando en forma especial el factor de la tecnología con la finalidad de garantizar la seguridad de la información y la continuidad de las operaciones, conscientes de la importancia que tiene la tecnología de información y el control interno dentro de la cadena de valor del negocio y en la estructura organizacional que la conforma.

Para una adecuada administración del riesgo existe una variedad de herramientas informáticas para dicho fin, de tal manera que se maximice el monitoreo y control de las operaciones, se mejore el control en el acceso a la información, se optimice la gestión de riesgos y auditoría interna y se proporcione información de calidad a la alta dirección para la toma oportuna de decisiones.

La presente tesis busca establecer un marco de control de gestión del riesgo operativo relacionado con la tecnología de información que sirva de guía para Directivos, Gerentes de TI, Auditores y Analistas de Riesgo en el desempeño de sus funciones dentro del gobierno y administración del riesgo tecnológico dentro de las Cooperativas de Ahorro y Crédito del Ecuador, tomando en consideración que se busca proteger los recursos financieros de los socios que han puesto su confianza en dicho sector financiero.

Índice General

Índice de Figuras

Índice de Tablas

ÍNDICE DE ABREVIATURAS

COAC'S	Cooperativas de Ahorro y Crédito
COBIT	Objetivos de Control para Tecnología de Información y Tecnologías relacionadas
COSO	Sponsoring Organizations of the Treadway Commission
DBA	Administrador de Bases de Datos
DBMS	Sistema de Administración de Bases de Datos
ISACA	Asociación para el Control y Auditoría de Sistemas de Información
ISACF	Fundación para el Control y Auditoría de Sistemas de Información
ISO	Organización Internacional de Normalización
ITGI	Instituto para el Gobierno de Tecnología de Información
ITIL	IT Library
LAN	Red de Área Local
SEI	Instituto de Ingeniería de Software
WAN	Red de Área Amplia

INTRODUCCIÓN

Luego de diversos eventos que ocurrieron hace casi una década, como los escándalos financieros que ocurrieron en Estados Unidos con las Instituciones Financieras y no Financieras que cotizaban en la Bolsa de Valores y la caída de las Torres Gemelas, a nivel mundial se formó una nueva corriente sobre la forma en que debe realizarse el Control Interno dentro de las Instituciones Financieras. Dicho Control Interno se basaba en el ***Riesgo***.

Riesgo es el daño potencial que puede surgir por un proceso presente o suceso futuro[1]. Sí, de acuerdo a esta definición podemos decir que el riesgo está latente en cualquier actividad o proceso que se realice sin que podamos determinar el momento de su ocurrencia pero sí realizar o tomar ciertas medidas preventivas para minimizar la probabilidad de ocurrencia y el impacto que esta pueda tener.

Las organizaciones sin importar su actividad o giro del negocio se enfrentan constantemente a diversos tipos de riesgos con los cuales deben convivir, sin que exista un mecanismo 100% confiable o seguro que permita evitar dichos riesgos.

En el caso de las Instituciones Financieras, el riesgo es parte integral dentro de las diversas operaciones que realizan, principalmente porque su materia prima fundamental es el dinero. El manejo del dinero proveniente de las captaciones es una responsabilidad demasiado alta para las instituciones financieras, debido a que para ellos representa la mayor parte de sus pasivos y deben tener la capacidad suficiente para poder almacenarlo, cuidarlo y después devolverlo a sus clientes.

En el Ecuador, luego del "remezón" que hubo a finales de los '90, durante la crisis financiera en el que muchos bancos considerados grandes cayeron, el sector financiero cooperativo a base de confianza y apoyo al microcrédito comenzó a escalar considerablemente hasta posicionarse como una parte importante dentro de la masa monetaria circulante en el País.

[1] Fuente: Wikipedia. http://es.wikipedia.org/wiki/Riesgo

Dicho crecimiento y revolución cooperativista ha ocasionado que dichas instituciones incorporen dentro de sus procesos de negocio, dos componentes muy importantes que para los bancos ya habían sido parte de su existir: la tecnología y la administración del riesgo.

Conscientes de la evolución de las cooperativas de ahorro y crédito, la Superintendencia de Bancos y Seguros comenzó a realizar controles más exhaustivos a las operaciones que estas realizaban y comenzó a delinear mecanismos de control básicos para garantizar su adecuado funcionamiento.

Poco a poco las COAC's dejaron de lado los procesos manuales y fueron incorporando diversas herramientas tecnológicas como bases de datos, computadores de última generación, redes privadas entre oficinas y hasta sistemas integrados de bancarización.

Por otro lado, la planificación y la toma de decisiones gerenciales que con muy buenos resultados, se basaba solamente en el manejo eficiente de la cartera y la liquidez, ahora debía considerar aspectos internos y externos que pudieran significar un riesgo. Es así, que aparecen dentro de la administración del riesgo: el riesgo de mercado, el riesgo de liquidez y el riesgo de crédito.

Sin embargo, en los últimos años se ha dado mucho énfasis al Riesgo Operacional, que busca entre otras cosas, minimizar el riesgo dentro de las operaciones del negocio, enfocándose además de los procesos, las personas y los eventos externos, en la base sobre la que se sustentan todos los procesos dentro de las COAC's: ***la tecnología***.

La presente Tesis tiene como uno de sus objetivos específicos, estudiar la forma en que las Cooperativas de Ahorro y Crédito han incorporado la tecnología dentro de sus procesos de negocio, la forma en que les ha permitido una eficiente toma de decisiones y sobre todo la manera en que esto ha significado un mejor servicio para sus clientes.

Así mismo, se busca establecer los lineamientos básicos para una adecuada gestión de los recursos tecnológicos tomando en consideración el riesgo operativo, los estándares internacionales y la legislación vigente en el País, buscando interrelacionarlos y determinando los aspectos que son aplicables y que podrían ser incorporados por las COAC's.

Además, se buscará establecer los mecanismos de control, herramientas y recursos disponibles para uso de gerentes, directores de tecnología, responsables de seguridad y auditores dentro de un ambiente de procesamiento electrónico de datos dentro de las COAC's.

Por consiguiente, la presente Tesis podría convertirse en una referencia para los diversos sujetos dentro de los procesos de negocio de las COAC's para una segura, eficiente y confiable gestión de tecnología de información que permita el desarrollo operacional y financiero de dichas instituciones en forma sustentable.

OBJETIVOS GENERALES DE LA TESIS

- Establecer los lineamientos de control para la Gestión Integral de Riesgos tecnológicos en las Cooperativas de Ahorro y Crédito del Ecuador bajo las normas internacionales vigentes y aquellas establecidas por la Superintendencia de Bancos y Seguros del Ecuador.

- Determinar la factibilidad de implementación a la que se enfrentan las Cooperativas de Ahorro y Crédito Ecuatorianas para la implementación de los controles de la gestión tecnológica bajo el marco de regulación gubernamental existente.

- Presentar la visión gerencial sobre la forma en que se implementa un adecuado gobierno de tecnología de información que agrega valor a los procesos de los diferentes niveles en la pirámide organizacional de las Cooperativa de Ahorro y Crédito Ecuatorianas.

OBJETIVOS ESPECÍFICOS DE LA TESIS

- Analizar el impacto que tienen los sistemas de información en el Sistema Financiero Cooperativo y su aprovechamiento dentro de sus operaciones así como en la toma de decisiones a nivel gerencial.
- Analizar la forma en que el control interno interviene dentro de la gestión de tecnología de información.
- Identificar los estándares, lineamientos y mejores prácticas relacionadas con una gestión de tecnología de información exitosa enfocada en la mitigación de los riesgos relacionados.
- Analizar la evolución y aplicación de las normas y lineamientos sobre la gestión del riesgo operativo por parte del Sistema Financiero Cooperativo.
- Establecer las diferentes variables que debe considerar una Cooperativa de Ahorro y Crédito para la implementación de los controles tecnológicos.
- Determinar la forma en que el control de interno interviene dentro de la cadena de valor de una Cooperativa de Ahorro y Crédito y el impacto que ésta genera.
- Analizar la forma en que las herramientas informáticas apoyan en la gestión del riesgo operativo tecnológico.
- Definir un Marco de Control Integral para la gestión del riesgo tecnológico dentro de las Instituciones Financieras del sector de cooperativas.

Capítulo 1.

Impacto de la Tecnología de Información en el Sistema Financiero Cooperativo

1.1. Evolución del Cooperativismo en el Ecuador y su impacto en el Microcrédito

1.1.1. Historia del Cooperativismo en el Ecuador

La historia del cooperativismo en el Ecuador, nace desde la época precolombina dentro del desarrollo cultural y económico del País, a través de las mingas y trabajos mancomunados que se formaron en el sector agrícola y campesino de las poblaciones incaicas.

Dichas agrupaciones de cooperación mutua tenían por objeto el beneficio social de sus miembros, sin perseguir algún fin de lucro particular y más bien se buscaba el desarrollo colectivo de la comunidad asociada. Dichas agrupaciones de colaboración social mutua existen hasta ahora en muchas poblaciones indígenas y campesinas del País.

A través de dicho modelo de colaboración comunitaria ya no se depende en forma paternalista del Estado para el desarrollo de los

sectores rurales o marginales; sino que por el contrario, se ha logrado su supervivencia y desarrollo económico y social a través del aporte voluntario y colaborativo de la comunidad en forma independiente y digna. Este modelo desarrollo es conocida como *economía solidaria.*

En general, se puede distinguir tres etapas dentro de la evolución del cooperativismo en el Ecuador: la etapa mutual, la primera Ley de Cooperativas; y, la ley Agraria y la segunda ley de Cooperativas.

1.1.1.1. La Etapa Mutual

En esta primera etapa, se formaron agrupaciones mutuales multifuncionales. En el caso de Guayaquil, en dichas agrupaciones intervenían diferentes grupos sociales y de la burguesía; mientras que en la Sierra la conformaban, bajo la dirección y patrocinio de la Iglesia Católica, obreros, artesanos, pequeños industriales, entre otros.

Los objetivos de estas agrupaciones tanto de la Sierra como de la Costa, eran apoyarse socialmente a través de la formación de centros de educación técnica, dispensarios y centros de abastos de productos de primera necesidad. Sin embargo, estas agrupaciones fueron perdiendo fuerza a medida que se formaron los sindicatos.

Adicionalmente, en esta etapa aparecen pequeñas organizaciones en Guayaquil como la Sociedad Protectora del Obrero en 1919 (considerada la primera Cooperativa del País); y en Riobamba, la Caja de Ahorro y Cooperativista de Préstamos de la federación Obrera del Chimborazo en 1927. No obstante, estas y otras organizaciones más que aparecieron, no contaban con servicios educativos y financieros, ni estructuras funcionales bien definidas, por lo que sus operaciones eran muy limitadas.

1.1.1.2. La Primera Ley de Cooperativas

En 1937 se sientan las bases del modelo cooperativista en el Ecuador, a través de la primera Ley de Cooperativas, bajo el gobierno del General Alberto Enríquez Gallo. A través de dicha ley se pretendía organizar y modernizar la estructura de producción campesina e indígena mediante la cooperación social, apareciendo de esta manera, las Cooperativas de Producción y las Cooperativas de Crédito como los pilares del desarrollo y fomento de la producción agrícola.

Se buscaba estimular al cooperativismo como un mecanismo que permita acabar con las desigualdades sociales y económicas en el sector agrícola; pero que sin embargo, dicha ley tenía demasiados vacíos legales y carecía de controles suficientes para regular la estructura y actividades de las agrupaciones sociales de aquella época. Aquello generó que sea aprovechado por personas con poder económico para adueñarse de las tierras, con el fin de lucrarse y aprovecharse de las exoneraciones fiscales existentes.

1.1.1.3. La Ley Agraria y la Segunda Ley de Cooperativas

En 1964 se expide la Ley de Reforma Agraria y Colonización con el objetivo de regular los procesos de adjudicación de tierras y establecer mejores controles en la conformación y funcionamiento de las cooperativas campesinas. Luego, en 1973 al expedirse la segunda ley Agraria, se mejoró la anterior ley y se buscó el desarrollo del sector agrícola y la modernización del cooperativismo agrícola en beneficio de las masas fomentándose el crédito para los campesinos y pequeños agricultores.

Durante 1966 se actualizó la Ley de Cooperativas con el objetivo de mejorar la formación, organización y actividad de las pequeñas cooperativas existentes para que se desarrolle en mejores condiciones el otorgamiento de préstamos destinados a la producción mediante la exoneración de impuestos y ciertas preferencias en la adquisición de maquinarias y adquisición de tierras. La última actualización a la Ley de Cooperativas se dio en 1992, sin que se hayan dado avances sustanciales al respecto.

1.1.2. Las Cooperativas de Ahorro y Crédito y su impacto en la Economía Ecuatoriana

Alrededor del año 1879, en la ciudad de Guayaquil, se fundó la primera Caja de Ahorro del País, a través de la *Sociedad de Artesanos Amantes del Progreso;* de ahí en adelante, se fundaron diversas cooperativas de ahorro y crédito y mutualistas dentro del marco de acontecimientos de la etapa mutual analizada anteriormente.

Es a partir de los años sesenta que comienza a tomar fuerza el sector cooperativo de ahorro y crédito y comienzan a aparecer instituciones sólidas y debidamente organizadas, tanto en el sector urbano como rural. Pero es a partir de los años ochenta, cuando la mayor parte de las cooperativas apuntan al sector urbano y sus miembros comienzan a pertenecer a las clases sociales media y media-alta, especialmente el sector de los educadores son quienes integran las cooperativas de ahorro y crédito de aquella época.

Ya a partir de los años noventa y luego de la crisis financiera de finales de aquella década, las Cooperativas de Ahorro y Crédito, fueron consolidándose como el segundo subsistema más fuerte dentro del Sistema Financiero Ecuatoriano, luego de los Bancos Privados.

Al 2007 la participación de las Cooperativas de Ahorro y Crédito dentro del Sistema Financiero se ha mantenido constante y crecido paulatinamente, tal es así, que al 2007 el Total de Activos fue del 4.9% respecto al resto del Sistema, reportándose 38 Cooperativas bajo el control de la Superintendencia de Bancos y Seguros.

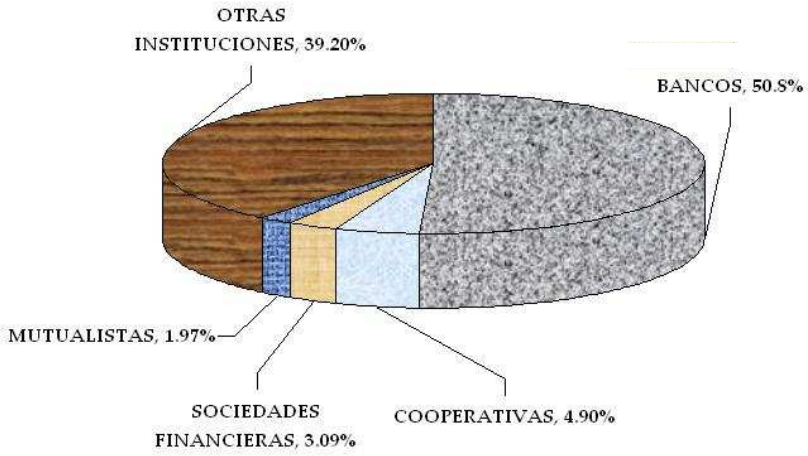


Figura 1.1 Porcentaje de Activos por Sector dentro del Sistema Financiero al 31 de Diciembre del 2007

Respecto a las captaciones de ahorros, las Cooperativas de Ahorro y Crédito han tenido un crecimiento importante en los últimos años, registrándose hasta el año 2007, un total de captaciones de 938 millones de dólares, mientras que las Mutualistas 435 millones de dólares y las sociedades financieras por un total de 350 millones de dólares.

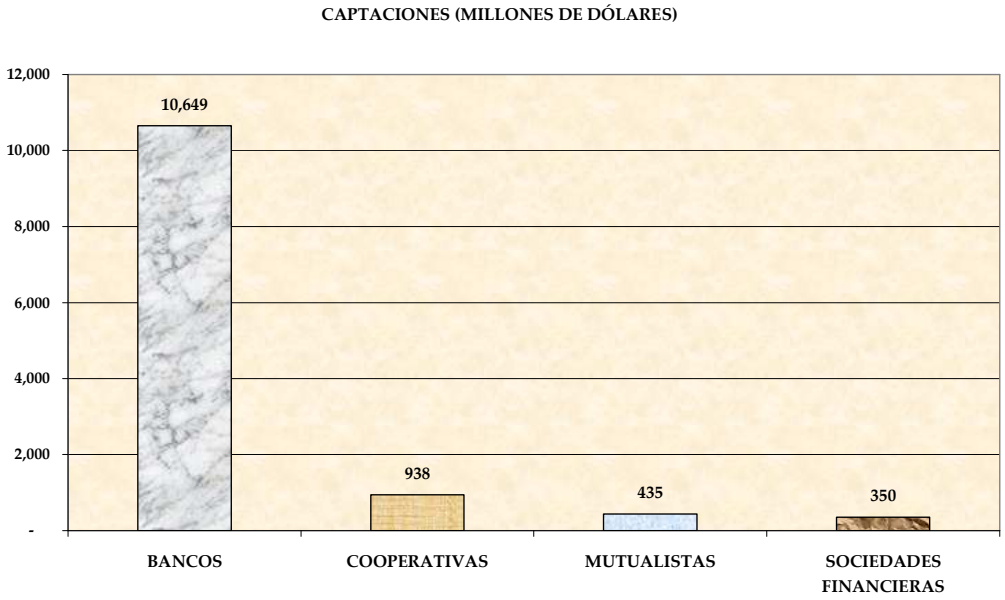


Figura 1.2. Total de Captaciones por Sector dentro del Sistema Financiero (A Diciembre 31 del 2007).

En cuanto a la Cartera de Crédito, cabe destacar que las Cooperativas de Ahorro y Crédito a diciembre del 2007 tenían una participación del 11% respecto al resto del Sistema Financiero por un monto de 1,012 millones de dólares. A continuación un gráfico demostrativo.

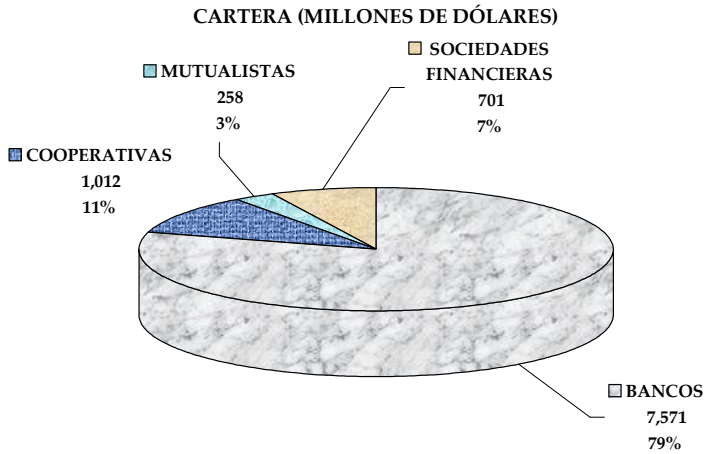


Figura 1.3. Total de Cartera de Crédito por Sector dentro del Sistema Financiero (A Diciembre del 2007).

En lo concerniente a la rentabilidad, las COAC's han demostrado un crecimiento importante, pero que todavía no ha sido lo suficiente

como para consolidarse como el segundo subsistema más rentable después de los bancos. Al 2007, las utilidades totales de las COAC's fue de 20.28 millones de dólares. A continuación se muestra un gráfico al respecto:

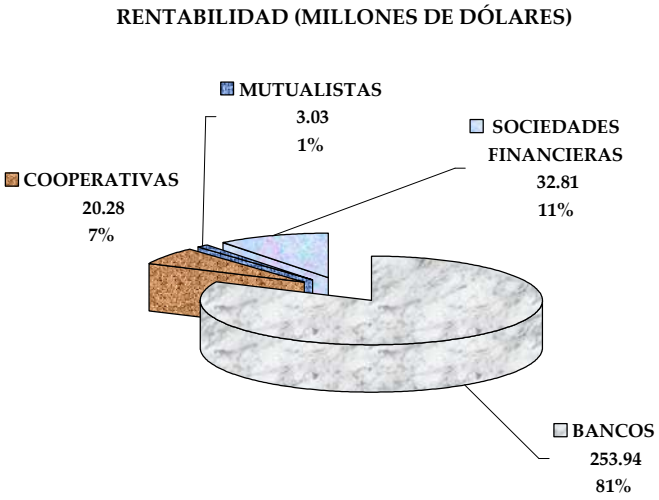


Figura 1.4. Total de Utilidades por Sector dentro del Sistema Financiero (A Diciembre del 2007).

Por lo tanto, se puede observar que las COAC's han tenido un crecimiento importante dentro del Sistema Financiero Nacional, a base de confianza, transparencia y apuntando hacia la función social.

Cabe destacar, que todavía existen centenares de COAC's que no están bajo el control de la Superintendencia de Bancos y sobre las cuales no existen estadísticas definidas respecto a sus principales indicadores. Sin lugar a dudas, luego de los bancos las COAC's se han consolidado como el subsistema financiero más importante dentro de la economía ecuatoriana.

1.1.3. El Microcrédito como fuente de desarrollo en el Ecuador

1.1.3.1. Qué son las Microfinanzas

De acuerdo a la CGAP[2], microfinanzas significa "la provisión de servicios bancarios a personas de menores ingresos, particularmente a los pobres y los muy pobres".

Bajo dicha definición se deriva el concepto de microcrédito como la colocación de recursos a través de préstamos para la realización de pequeños negocios informales de microempresarios.

Sin embargo, vale recalcar que los clientes que acceden a los microcréditos no son necesariamente microempresarios, sino que involucra a todo tipo de clientes entre ellas, personas pobres que utilizan los servicios financieros para enfrentar emergencias, mejorar sus casas y afrontar otros tipos de obligaciones.

Dichas personas también acceden a toda una gama de servicios financieros como son la apertura de cuentas de ahorros, inversiones en depósitos a plazo fijo, transferencias interbancarias, remesas del exterior, cajeros automáticos y hasta acceso a cuentas corrientes y operaciones por Internet.

Actualmente, en el negocio de las microfinanzas intervienen bancos, cooperativas de ahorro y crédito, mutualistas, entre otras.

[2] El CGAP (Grupo Consultivo de ayuda a la Población más Pobre), está conformado por 29 agencias donantes internacionales que apoyan a las microfinanzas.

1.1.3.2. Principios de las Microfinanzas

De acuerdo a la CGAP y sus 33 miembros cooperantes, existen 11 principios clave de las Microfinanzas y que son presentadas a continuación:

1. Las personas de escasos recursos necesitan una variedad de servicios financieros no sólo préstamos.
2. Las microfinanzas representan una herramienta poderosa en la lucha contra la pobreza.
3. Las microfinanzas se refieren a la creación de sistemas financieros que atiendan las necesidades de las personas pobres.
4. Las microfinanzas pueden y deben ser sostenibles si se espera alcanzar a un gran número de personas pobres.
5. Las microfinanzas requieren la construcción de instituciones financieras locales y permanentes.
6. El microcrédito no es siempre la solución.
7. Los techos a las tasas de interés pueden perjudicar el acceso de las personas pobres a créditos.
8. El papel desgobierno es uno de facilitador, no el de un proveedor directo de servicios financieros.
9. Los fondos de los cooperantes deben complementar en vez de competir con el capital del sector privado.
10. La limitación crucial es la insuficiencia de instituciones sólidas y de gerentes calificados.
11. Las microfinanzas funcionan mejor cuando se revela y mide su desempeño.

1.1.3.3. El Microcrédito en el Ecuador

En el Ecuador el desarrollo de las microfinanzas ha sido destacado en relación a los demás países de la región. Dentro de dicho mercado, bancos cooperativas, sociedades

financieras y ONG's brindan diferentes servicios micro financieros.

El Estado y las instituciones gubernamentales llamadas a aquello, han promovido y demostrado la intención de impulsar las microfinanzas pero sin que se establezcan todavía estrategias y políticas claras al respecto y que además, se asegure un ambiente propicio para el desarrollo de las microfinanzas en el Ecuador bajo un mercado de libre competencia.

Las regulaciones y controles gubernamentales, a pesar de mostrar cierta flexibilidad, en ocasiones podría ser muy restrictiva para muchos microempresarios y por consiguiente, les impida llegar a obtener microcréditos oportunamente.

Las instituciones pequeñas que se han especializado en el campo del microcrédito han comprendido la importancia de la innovación tecnológica y de la forma en que esta les permite realizar una adecuada planificación estratégica y el acceso a recursos que les permita ofrecer nuevos productos y servicios; así como garantizar la seguridad de la información y ser más competitivos.

1.1.4. El Cooperativismo y su incidencia en el microcrédito

1.1.4.1. Ranking de las principales Cooperativas del Ecuador

Dentro del sector cooperativo, existen Entidades Financieras con muy buena calificación de riesgo, entre las que a Diciembre del 2008 se destacan: la Cooperativa Nacional y la CACPECO con una calificación de AA- a Diciembre del 2008.

No obstante, existen otras Cooperativas que también destacan debido a que presentan una alta calidad en sus activos, eficiencia administrativa, rentabilidad, liquidez y suficiencia de capital; tales como: Juventud Ecuatoriana, 29 de Octubre, OSCUS, Andalucía, San Francisco y el Sagrario.

Para un mayor detalle sobre la calificación de riesgo de las COAC's, sírvase revisar la página Web de la Superintendencia de Bancos a través del link: https://www.superban.gov.ec/pages/info_calificacion_7.htm#5. Así mismo, existen boletines financieros emitidos en forma mensual en donde se puede analizar el comportamiento y resultados financieros de las COAC's a través del link: https://www.superban.gov.ec/pages/c_cooperativas_boletines.htm.

1.1.4.2. Participación de las Cooperativas en el Microcrédito

En el Ecuador existe una asociación de instituciones financieras y ONG's denominada Red Financiera Rural (RFR); la misma que tiene como objetivo promover y apoyar el desarrollo del microcrédito en el País, sobre todo en las zonas rurales y a poblaciones menos favorecidas.

A través de dicha organización, sus integrantes han logrado importantes avances en el campo del microcrédito a través de capacitación, eventos y programas de gerenciamiento integral de microfinanzas, foros y talleres de trabajo sobre nuevas normativas legales por entrar en vigencia.

En forma periódica y regular esta organización pone a disposición de sus miembros, información estadística y financiera de sus miembros y presenta benchmarking entre

los diferentes sectores que integran el sistema financiero local y latinoamericano.

De acuerdo a información de la Superintendencia de Bancos, al 30 de Junio del 2008, se dio un total de 1,2 millones de dólares en operaciones de microcrédito con un crecimiento del 9.1% frente al mismo periodo el año anterior. A continuación la participación de las instituciones financieras en operaciones de microcrédito de acuerdo a cada sector:

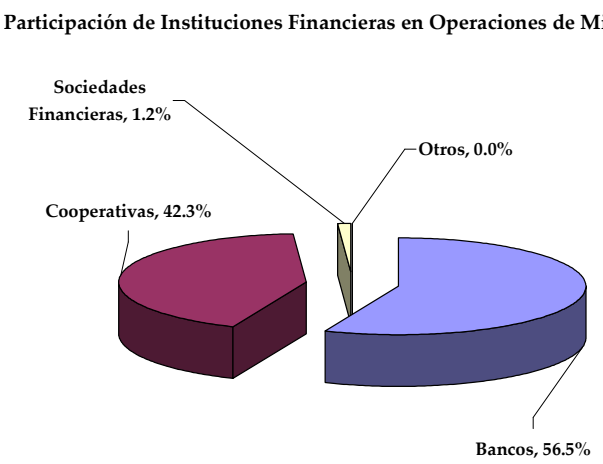


Figura 1.5. Operaciones de Microcrédito por Subsistema a Dic. Al 30 de Junio del 2008 (Fuente: Superintendencia de Bancos).

Como se puede observar, las COAC's tienen el 42% de la participación del sector financiero en operaciones de microcrédito. Aquello, es muy significativo considerando el volumen de crédito que generan los bancos privados.

Esto refleja que las COAC's tienen una participación muy alta en el otorgamiento de créditos a microempresarios y personas de clase media baja para el emprendimiento de nuevos negocios o el mejoramiento de las condiciones de vida de aquellas personas.

Sin embargo, dada la crisis financiera en los Estados Unidos y el manejo de las tasas de interés en el Ecuador, para los bancos privados va a ser más rentable colocar dinero en operaciones de microcrédito a pesar que el costo y riesgo en ese tipo de operaciones aumenta, lo que ocasionará una fuerte competencia para las cooperativas.

Por ello, las cooperativas deberán generar nuevas estrategias que les permita mantener y aumentar su participación en el

mercado y poder hacer frente a la competencia de los bancos privados. Las COAC's deberán preocuparse de lo siguiente:

- Generar nuevos productos y servicios enfocados al microcrédito con una adecuada base y sustento técnico - financiero.
- Ser más eficientes y disminuir sus costos operativos.
- Innovar constantemente haciendo uso de la tecnología para mejorar el servicio y atención de sus clientes.
- Masificar sus operaciones dentro de mercados aún no explotados por la competencia.
- Mejorar sus controles y seguridad de la información para generar confianza en sus depositantes al mejorar sus calificaciones de riesgo.
- Fidelizar a sus clientes a través de la creación de líneas de crédito renovables.
- Ser competitivos en el manejo de tasas de interés, montos de crédito y plazos.
- Disminuir las condiciones de apertura de cuentas pero bajo controles adecuados para la prevención de Lavado de Activos.
- Asociarse entre entidades para el desarrollo de sus plataformas tecnológicas, integración de servicios y cobertura colaborativa.

1.2. Incorporación de la tecnología de información a los procesos de negocio de las COAC's.

1.2.1. Aplicación de la tecnología en la generación de nuevos productos y servicios en las COAC's.

Por muchos años, los bancos privados eran las únicas instituciones financieras que hacían un alto uso de la tecnología para el manejo de sus operaciones y prestación de servicios, debido en gran medida en su alta capacidad adquisitiva en nuevas tecnologías.

Mientras tanto, las COAC's y demás tipos de instituciones financieras se limitaban a hacer un uso muy básico de la tecnología debido a sus bajos recursos y la falta de una percepción clara sobre su uso y la falta de confianza en ella y de sus clientes, asociando la innovación como un costo innecesario y encarecimiento de los servicios prestados respectivamente.

Sin embargo, desde hace un poco más de una década, las COAC's y demás tipos de instituciones financieras se han dado cuenta de la eficiencia y utilidad que se puede obtener bajo el uso de tecnología y que a más de ser un costo, es una inversión. Tal es así, que en la actualidad existen instituciones que ofrecen casi los mismos servicios que ofrecen los bancos privados, como cuentas corrientes, cajeros automáticos, transacciones por Internet y hasta servicios financieros por vía móvil.

Incluso, muchas COAC's han iniciado proyectos de gestión de la información a través de "cero papeles" mediante la implementación de sistemas de gestión documental que se integran dentro de cada uno de los procesos de la entidad, desde la apertura de las cuentas de ahorros, pasando por la generación de créditos y manejo de cartera hasta el manejo de la información contable y tributaria.

Todas estas innovaciones han permito inadecuado crecimiento en el número de sus clientes y un mejor servicio para ellos; un manejo eficiente de la información; un control operativo más detallado y crear nuevas estrategias de negocios.

Vale resaltar, que las principales COAC's disponen de Servidores robustos de bases de datos y de administración de dominio, equipos de conmutación y enrutadores con tecnología de punta y hasta centros de cómputo alternos para hacer frente a contingencias graves. Esto demuestra que ha habido una importante evolución en la forma de

planificar y administrar los recursos tecnológicos por parte de la alta gerencia en este tipo de Instituciones.

En este sentido, la Superintendencia de Bancos y Seguros ha sido un factor muy preponderante para dicha evolución, ya que a través de talleres, seminarios de capacitación, las auditorías anuales y las revisiones especiales, han enfatizado a las COAC's sobre la adopción de mejores prácticas en la administración de la Tecnología de Información.

Actualmente, se cuenta con muchas directrices en forma de leyes, decretos, codificaciones, circulares y oficios generadas a través de dicho ente regulador para que las COAC's cumplan con una administración de sus recursos de TI y evalúen los riesgos a los cuales están expuestos, sobre todo en lo relacionado con el riesgo operativo.

1.2.2. Planeación estratégica organizacional apoyada por la tecnología dentro de las COAC's

En la actualidad las COAC's en forma progresiva han ido incorporando a sus procesos de planeación estratégica, paquetes informáticos que les ha permitido realizar entre otras cosas, análisis de la competencia, estudio del mercado financiero, análisis de la situación crediticia de sus clientes, administración de riesgos, benchmarking financiero y hasta proyecciones estadísticas del sistema financiero bajo diferentes variables y escenarios.

En este sentido, ha sido muy importante el aporte de instituciones como la Red Financiera Rural, CAEFIC, y los burós de información crediticia como Credit Report (uno de los más destacados por los servicios de valor agregado que ofrecen); las cuales, a través de capacitación, asesoría y productos de software financiero y de administración de riesgos han ayudado a mejorar la toma de decisiones de los gerentes y mandos medios de las COAC's.

No obstante, hay que reconocer que todavía existen COAC's que por la falta de recursos, no pueden acceder a paquetes informáticos especializados que les permita en forma automatizada realizar sus planes estratégicos. Sin embargo, hacen uso de herramientas ofimáticas como hojas de cálculo para dicho cometido.

Capítulo 2.

El Control Interno dentro del Gobierno de Tecnología de Información: Análisis de los Lineamientos y Estándares vigentes

2.1. Estándares vigentes para el Control Interno de TI

En la actualidad existe una variedad de lineamientos y mejores prácticas para el control y administración de la tecnología de información; los cuales algunos de ellos, han ido madurando a través del tiempo hasta convertirse en verdaderos estándares de uso obligado dentro de la gestión de TI.

ESTÁNDAR	ORGANISMO EMISOR
COBIT (Objetivos de Control para tecnología de información y tecnología relacionada)	**ISACA** (Asociación de Auditoría y control de Sistemas de Información).
DESCRIPCIÓN:	
Este es un estándar internacional de referencias de Auditoría informática, que abarca "las mejores prácticas" de gobierno y auditoría de tecnología de información. A través de dichos objetivos de control, los diferentes Usuarios de TI desde la Alta Gerencia hasta los niveles operativos pueden comprender y administrar los riesgos relacionados con la tecnología de información, permitiéndoles establecer una interrelación entre los procesos de administración, tecnología, control interno y análisis de riesgos. Para mayor información visite: http://www.isaca.org/	
ISO 17799 e ISO 27000 (Estándares de Administración de Control y Seguridad de la Tecnología de Información)	**ISO** (Organización Internacional de Estándares)

DESCRIPCIÓN:
Ambos estándares pertenecen a la familia de los ISO, el uno como precedente del otro y presentan "las mejores prácticas" para la implementación de un Sistema de Control y Seguridad de Tecnología de la Información. Se estructuran en diferentes áreas de control. Para mayor información visite: http://www.iso.org/iso/home.htm

ITIL (Librería de Infraestructura de TI)	**OGC y CCTA** (Oficina de Comercio Gubernamental y la Central Computer and Telecommunications Agency, del Reino Unido).

DESCRIPCIÓN:
La Biblioteca de Infraestructura de Tecnologías de Información consiste en un "Framework" (marco de trabajo) que encierra las mejores prácticas para proporcionar una adecuada entrega de servicios de tecnologías de la información dentro de las organizaciones. Abarca un amplio conjunto de procedimientos de gestión de TI formulados para facilitar a las organizaciones altos niveles de calidad y eficiencia en sus operaciones de TI, abarcando la infraestructura, desarrollo y operaciones de TI. Para mayor información visite: http://www.itil.co.uk/

CMMI (Integración del Modelo de Evolución de Capacidades de software)	**SEI** (Instituto de Ingeniería de Software)

DESCRIPCIÓN:
CMMI es un modelo enfocado hacia la evaluación de la capacidad o habilidad que tiene una organización para planificar, desarrollar y mantener Sistemas de Información. Se divide en 5 aspectos de análisis y 18 áreas de evaluación u objetivos de control, semejantes muchos de ellos a los que presenta COBIT. Para mayor información visite: http://www.sei.cmu.edu/cmmi/

SSE – CMM (Ingeniería de Seguridad de Sistemas – Modelo de Madurez de Capacidades)	**NSA** (Agencia de Seguridad Nacional con el apoyo de la Universidad de Carnegie Mellon)

DESCRIPCIÓN:
A través de este modelo se recogen las metodologías más utilizadas por las organizaciones en la elaboración de sus Sistemas de Seguridad informática, a través de una descripción de las características principales que debe tener la estructura de seguridad de TI y telecomunicaciones en las organizaciones. Para mayor información visite: http://www.sse-cmm.org/index.html

SYSTRUST (Principios y Criterios de Confiabilidad de Sistemas)	**AICPA** y **CICA** ("Asociación de Contadores Públicos" y el "Instituto Canadiense de Contadores Certificados")

DESCRIPCIÓN:

Estos principios pretenden incrementar la confianza de la alta gerencia, clientes y socios, con respecto a la confiabilidad en los sistemas por una empresa o actividad en particular. Este modelo incluye elementos como: infraestructura, software de cualquier naturaleza, personal especializado y usuarios, procesos manuales y automatizados, y datos. El modelo persigue determinar si un sistema de información es confiable, (i.e. si un sistema funciona sin errores significativos, o fallas durante un periodo de tiempo determinado bajo un ambiente dado).

Para mayor información visite:
http://infotech.aicpa.org/Resources/Trust+Services/Resources_Home.htm

"Administración del Control de Datos de la Tecnología de Información"	**CICA** (Instituto Canadiense de Contadores Certificados)

DESCRIPCIÓN:

Este es un modelo basado en el concepto de perfiles y roles. Esta establece responsabilidades relacionadas con los controles y seguridades de la tecnología de información. Esta norma clasifica los roles en los siguientes grupos:

- A Nivel Interno: Alta Dirección, Gerencia General, Gerencia de Sistemas, Jefes Departamentales, Supervisores y usuarios.
- A nivel Externo: Proveedores, Desarrolladores y Soporte Técnico.

Por otro lado, establece una diferenciación entre autoridad y responsabilidad respecto al control y riesgo de la tecnología de información. Esta norma se compone de objetivos de control y "prácticas generalmente aceptadas".

Para mayor información visite: http://www.cica.ca/index.cfm?ci_id=17150&la_id=1

"Administración de la inversión de tecnología de Inversión: un marco para la evaluación y mejora del proceso de madurez"	**GAO** (Oficina de Contabilidad General de los Estados Unidos)

DESCRIPCIÓN:

Dicho modelo está basado en la identificación de los procesos críticos de la organización, analiza la importancia de las inversiones en tecnología de información y comunicación de datos.

Para mayor información visite: http://www.gao.gov/

"Administración de Sistemas de Información: Una herramienta de evaluación práctica"	Directiva de Recursos de Tecnología de Información. (Information Technology Resources Board)

DESCRIPCIÓN:

Es un modelo orientado hacia el e-governance, que permite a las instituciones gubernamentales llegar a una profunda comprensión de la implementación estratégica de Tecnología de Información y negocios electrónicos que permita un desarrollo sustentable del sector público, un mejoramiento en la eficiencia y eficacia de los servicios públicos y la generación de nuevas oportunidades de servicios acorde con las metas estratégicas gubernamentales.

Para mayor información visite: http://www.access-board.gov/	
"Guía para el Cuerpo de Conocimientos de Administración de Proyectos"(PMBOK)	Comité de Estándares del Instituto de Administración de Proyectos
DESCRIPCIÓN:	
Esta es una guía que se basa en "las mejores prácticas" sobre administración de proyectos de tecnología de información. Esta guía incluye los elementos necesarios para una adecuada gestión de proyectos, explicando las metodologías más utilizadas por los expertos para una exitosa implementación de proyectos de TI y que abarca: • Gestión de la Integración de Proyectos, • Gestión del Alcance en Proyectos, • Gestión del Tiempo en Proyectos, • Gestión de la Calidad en Proyectos, • Gestión de Costos en Proyectos, • Gestión del Riesgo en Proyectos, • Gestión de Recursos Humanos en Proyectos, • Gestión de la Comunicación en Proyectos, y • Gestión de la Procura (Logística) en Proyectos. Para mayor información visite: http://www.pmi.org/Pages/default.aspx	
"Administración de Seguridad de Información: Aprendiendo de Organizaciones Líderes"	GAO (Oficina de Contabilidad General de los Estados Unidos)
DESCRIPCIÓN:	
Dicho modelo presenta las 16 prácticas esenciales para la implementación de un sistema de seguridad de TI, basado en el análisis de las metodologías empleadas por las ocho organizaciones privadas líderes en el mundo respecto a seguridad del área PED. Para mayor información visite: http://www.gao.gov/	

Tabla 2.1. Estándares Internacionales sobre Seguridad de TI

Como vemos, la mayoría de estos estándares y guías se basan en las "prácticas aceptadas" de las organizaciones y expertos de tecnología de información; lo cual, significa que están desarrolladas de acuerdo a la realidad de las organizaciones y que ya han sido probadas con éxito en empresas exitosas a nivel mundial. Esto garantiza la disposición de herramientas eficaces para la implementación de los Sistemas de Control y Seguridad informática por parte de los profesionales y auditores de TI.

2.2. El Gobierno de Tecnología de Información a través de COBIT

2.2.1. ISACA y el *e-governance*

ISACA por sus siglas en inglés, significa: Asociación en Control y Auditoría de Sistemas de Información; la misma que desde su fundación en 1969 tiene como objetivo asociar a los profesionales de diferentes áreas que están relacionados o participan en la práctica de administración, control y auditoría de tecnología de información. Dicha organización nació con el nombre de EDP Auditors Association (Asociación de Auditores de Procesamiento Electrónico de Datos) y actualmente cuenta con más de 75,000 miembros en más de 160 países.

Entre los miembros de ISACA existen profesionales ingenieros en sistemas, auditores en control de gestión, economistas, contadores públicos, ingenieros comerciales, entre otros, lo cual es una prueba de que para ser parte de esta reconocida asociación no se requiere necesariamente ser un profesional en el área de sistemas pero sí que tenga un desarrollo profesional o tenga interés en dicha área.

La misión de ISACA es "soportar los objetivos empresariales mediante el desarrollo, promoción y entrega de investigaciones, estándares, competencias y prácticas para un efectivo gobierno, control y evaluación de los sistemas de información y la tecnología relacionada"; tal es así que esta organización cada año se ha preocupado por mantener actualizado a los gerentes, auditores y profesionales de tecnología de información, en el manejo adecuado de los recursos informáticos, la seguridad de la información y la implementación de proyectos de TI, de acuerdo a las "mejores prácticas".

Actualmente, ISACA cuenta con alrededor de 175 capítulos en 70 países de todo el mundo, entre los que se encuentra el capítulo Quito-

Ecuador que fue aceptado el 6 de septiembre de 2002 y está conformado por profesionales en diferentes áreas quienes se han asociado con el propósito de desarrollar y promover la Auditoría de Sistemas de Información en nuestro País de una manera dinámica y reconocida. Actualmente este capítulo se encuentra en fase de consolidación mediante la realización de algunas actividades entre las que podemos mencionar:

- Incorporación de nuevos miembros buscando ampliar su cobertura y fortalecerse como organización.
- Facilitar e instruir a los participantes en la presentación del examen CISA.
- Difusión de actividades y eventos de capacitación en COBIT y gobierno de TI.
- Lograr alianzas estratégicas con empresas líderes en el campo de la seguridad y riesgo informático para la prestación de servicios de valor agregado.

En 1998 ISACA fundó el IT Governance Institute (ITGI), la misma que tiene como objetivo apoyar a la alta dirección en el liderazgo empresarial, para asegurar un éxito constante y duradero al ampliar la conciencia acerca de la necesidad y el beneficio de un manejo adecuado de las TIC.

Este Instituto desarrolla y promueve la comprensión de lo importante que es el vínculo entre las TIC y el manejó de una empresa, y ofrece una guía sobre las mejores prácticas aplicables al manejo de los riesgos relacionados con las TIC, a través de lo que ellos llaman el IT Governance. Esta es una filosofía empresarial de gobierno de la Tecnología de Información en el que se busca una participación activa de la gerencia en los procesos de TI, su desarrollo y Control; a través de la alineación de la estrategia de las TIC's con las operaciones de las organizaciones, la difusión de estrategias y metas a nivel de toda la organización, la estructuración de las organizaciones hacia el logro de

las metas y objetivos y la adopción e implementación de una estructura de control de la TI acompañado de una adecuada medición de su desempeño.

Los resultados que se esperan al establecer esta filosofía del IT Governance, son los siguientes:

1. Que la TI esté alineada con la empresa y produzca los beneficios prometidos.
2. Que la TI habilite a la empresa al explotar oportunidades y generar los máximos beneficios.
3. Que se mida el desempeño de los procesos de Ti en forma eficiente y continua.
4. Que los recursos de la TI se empleen responsablemente.
5. Que los riesgos relacionados con la TI se manejen adecuadamente.

2.2.2. Áreas de acción para la gestión de TI

El IT Governance define cinco áreas de acción que se deben considerar en el manejo de la tecnología de información:

- **Alineación estratégica de la Tecnología de Información.-** Los recursos planificados para la inversión en TI deben estar alineados a los objetivos estratégicos de la organización, aunque en la realidad esto no se cumpla por completo. Es decir, la estrategia de TI debe ser parte de la estrategia global de la organización y ser un soporte para las operaciones de la organización.

- **Valor derivado de Tecnología de Información.-** La TI para una organización debe significar una ventaja competitiva, un mejoramiento a la eficiencia de sus operaciones, una mayor satisfacción del cliente, mayores rendimientos y utilidades,

mejor manejo de la información y la toma de decisiones correctas y oportunas.

- **Administración de Recursos.-** Es necesario que se realice una adecuada administración de los recursos tecnológicos con el objetivo de garantizar una adecuada inversión, basado en una relación costo – beneficio que favorezca a la organización considerando a la aplicaciones, infraestructura, información y las personas, optimizando el conocimiento y la infraestructura.

- **Medición del desempeño.-** Se requiere definir una serie de parámetros sobre los cuales se debe desarrollar el manejo o administración de la TI. Esto deberá servir para medir el desempeño de la TI dentro de las organizaciones y si es que se están cumpliendo las metas y objetivos institucionales. La mejor manera de efectuar este tipo de medición, es mediante alinear los parámetros de cumplimiento de TI con los de la organización, de tal forma que se pueda establecer una relación entre el desempeño, eficiencia y productividad de la organización con la gestión de TI.

- **Manejo de Riesgos.-** La administración además de preocuparse por los riesgos operacionales y financieros a los que está expuesta la organización, debe poner especial interés en determinar, analizar y minimizar los riesgos relacionados con el manejo de la TI, debido principalmente a que un aumento del riesgo de amenazas para la TI de la organización, podría ocasionar simultáneamente un aumento del riesgo de las operaciones y gestión financiera de la organización.

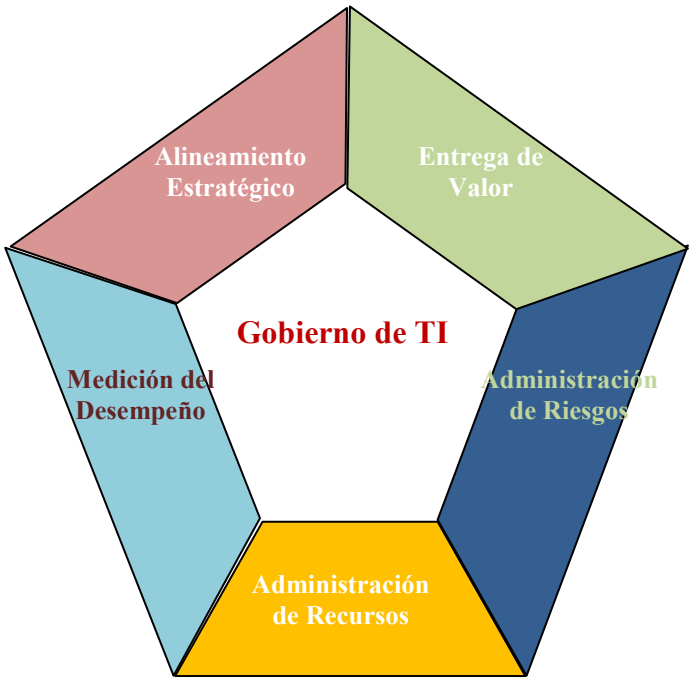


Figura 2.1. Áreas de Enfoque del gobierno de TI. (Fuente: ISACA)

2.2.3. Los Objetivos de Control de COBIT

COBIT en su versión 4 define una serie de objetivos de control enfocados a la administración y control de la tecnología de información dentro de cualquier organización bajo ambientes de procesamiento electrónico de datos bajo las directrices del marco definido por el IT governance. A continuación se presenta la forma en que ha evolucionado COBIT:

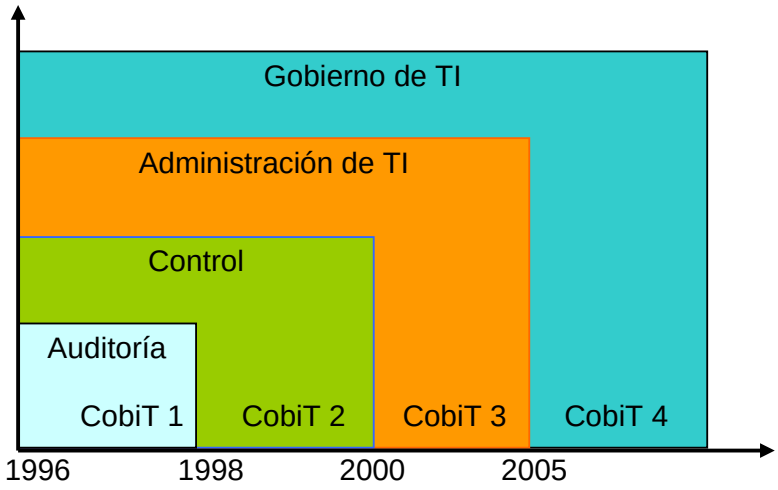


Figura 2.2. Evolución de COBIT

Cada uno de estos objetivos de control están bajo cuatro dominios; pero a su vez, los objetivos de control se definen en objetivos de control de alto nivel y objetivos de control de bajo nivel (llamados también actividades hasta la versión 3 de COBIT). A continuación se detallan los Objetivos de Control de Alto Nivel de COBIT:

DOMINIO	OBJETIVOS DE CONTROL
Planificación y Organización.-Este dominio se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos de negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.	• PO1. Definir un plan estratégico de TI • PO2. Definir la arquitectura de información • PO3. Determinar la dirección tecnológica • PO4. Definir los procesos, organización y relaciones de TI • PO5. Administrar la inversión de TI • PO6. Comunicación de la directrices Gerenciales • PO7. Administración del Recurso Humano de TI • PO8. Administrar con Calidad • PO9. Analizar y Administrar Riesgos • PO10. Administración de Proyectos

Adquisición e Implementación.- Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a los sistemas existentes.	• AI1. Identificación de soluciones automatizadas • AI2. Adquisición y mantenimiento de Software de aplicación • AI3. Adquisición y mantenimiento de la infraestructura tecnológica • AI4. Facilitar la Operación y el Uso • AI5. Proveer Recursos de TI • AI6. Administración de Cambios • AI7. Instalar y Acreditar soluciones y cambios
Prestación y soporte.- En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.	• DS1. Definir y administrar del nivel de servicio • DS2. Administrar servicios de terceros • DS3. Administrar el desempeño y la capacidad • DS4. Asegurar el servicio continuo • DS5. Garantizar la seguridad de los sistemas • DS6. Identificación y asignación de costos • DS7. Educar y Entrenar a los Usuarios • DS8. Administrar la Mesa de Servicio y los Incidentes • DS9. Administración de la configuración • DS10. Administración de problemas e incidentes • DS11. Administración de datos • DS12. Administración del Ambiente Físico • DS13. Administración de Operaciones
Monitoreo y Seguimiento.- Todos los procesos de una organización necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los	• ME1. Monitorear y Evaluar el desempeño de TI • ME2. Monitorear y Evaluar el Control Interno • ME3. Asegurar el cumplimiento de requerimientos Externos

requerimientos de control, integridad y confidencialidad.	• ME4. Proveer gobierno de TI

Tabla 2.2. Objetivos de Control de COBIT

2.2.4. Aplicación de COBIT 4 en las organizaciones

COBIT 4 es un compendio muy amplio de mejores prácticas y lineamientos para una adecuada administración de TI, pero que en la práctica es demasiada compleja su aplicación sobre todo en organizaciones muy pequeñas o medianas en donde no existen formalmente definidos sus procesos o carecen de los recursos eficientes para un adecuado control de TI.

Sin embargo, dependiendo de cada organización, puede hacerse uso de sus principales objetivos de control, de tal manera que se pongan en práctica los objetivos de control que más se adapten a las necesidades y requerimientos de la organización.

2.3. La prestación de servicios tecnológicos utilizando ITIL

Dentro de las organizaciones, ya sean estas medianas o grandes, el Departamento de TI cumple un papel fundamental dentro de la entrega de servicios y soporte para la ejecución de los procesos dentro de ambientes de procesamiento electrónico de datos. Es importante que la alta dirección preste mucha atención a la forma en que se realiza dicho soporte considerando que para el área de TI los demás departamentos y Usuarios son sus clientes.

A través de ITIL, actualmente en la versión 3, se establece la dirección sobre la que debe basarse un adecuado soporte y servicio de TI ya que pone de manifiesto un conjunto de mejores prácticas que además de tratar los procesos y requerimientos técnicos y operacionales, también se relaciona con la gestión

estratégica, la gestión de operaciones y la gestión financiera de una organización moderna.

ITIL V.3 se compone de los siguientes libros que representan a cada una de las fases dentro del Ciclo de Vida de los Procesos de TI:

- ***Estrategia de Servicio.-*** Esta es la fase en donde se diseña, desarrolla e implementa la gestión del servicio a nivel estratégico.

  Comprende los siguientes procesos:
  - Generación de Estrategias
  - Gestión del Portafolio de Servicios
  - Gestión de la Demanda
  - Gestión Financiera

- ***Diseño del Servicio.-*** En esta fase se define la arquitectura, los procesos, políticas y documentos en base con los requerimientos del negocio y alineado a los requerimientos futuros.

  Comprende los siguientes procesos:
  - Gestión del Catálogo de Servicios
  - Gestión del Nivel de Servicio
  - Gestión de la Capacidad
  - Gestión de la Disponibilidad
  - Gestión de la Continuidad del Servicio de TI
  - Gestión de la Seguridad de la Información
  - Gestión de Proveedores

- ***Transición del Servicio.-*** Es la fase previa a la puesta en producción de los nuevos servicios o aquellos modificados, en donde son desarrollados o mejorados en base a niveles óptimos de calidad.

Comprende los siguientes procesos:

- Planificación y Soporte de la Transición
- Gestión de Cambios
- Gestión de la Configuración y Activos del Servicio
- Gestión de Entregas y Despliegues
- Validación y Pruebas del Servicio
- Evaluación
- Gestión del Conocimiento

- ***Operación del Servicio.-*** Esta es la fase de puesta en producción y operación de los servicios de TI en donde se busca su eficiencia, eficacia y control de tal manera que genere valor para la organización.

  Comprende los siguientes procesos:

  - Gestión de Eventos
  - Gestión de Incidentes
  - Gestión de Peticiones
  - Gestión de Problemas
  - Gestión de Accesos
  - Monitorización y Control
  - Operación de TI
  - Centro de Servicio al Usuario

- ***Mejora Continua del Servicio.-*** En esta fase se busca el mejoramiento continuo de los servicios de TI de tal manera que se logre mantener un alto nivel de calidad y desempeño.

  Comprende los siguientes procesos:

  - Proceso de Mejora del Ciclo de Vida del Servicio
  - Informes del Servicio

A continuación se presenta en forma gráfica su estructura:

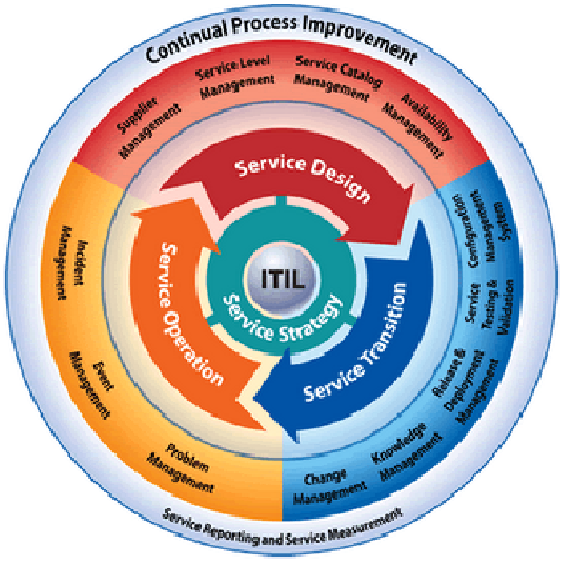


Figura 2.3. Estructura de ITIL V3

Como se puede ver, ITIL resume en forma clara y concreta el ciclo de vida de los servicios de tecnología de información, de tal forma, que los procesos de la organización basados en TI, sean eficientes, eficaces y sobre todo que generen valor a la organización y que pueda ser percibido por quienes hacen uso de los servicios de TI.

En el caso de las COAC's, el uso de ITIL les permitiría de sobre manera mejorar sus procesos de TI; sobre todo, les ayudaría a formalizar y mantener la calidad de los servicios de TI; el mismo que dentro de las regulaciones de la Superintendencia de Bancos, es esencial dentro de la administración del riesgo operativo.

2.4. La Seguridad de la Información de acuerdo a ISO 27000

2.4.1. La familia ISO 27000

La familia de las ISO 27000 (todavía en fase de desarrollo), es un conjunto de normas enfocadas hacia la administración de la seguridad

de la tecnología de información. En dicha serie de normas se destacan las siguientes:

- **ISO 27001**

  Esta Norma establece los ***requisitos*** para un adecuado Sistema de Gestión de la Seguridad de la Información (SGSI); por tanto, a través de dicha Norma se realiza la ***certificación*** de calidad en la gestión de seguridad de la información para las empresas que así lo deseen.

- **ISO 27002**

  Dicha Norma nació de la ISO 17799:2005 el 1 de Julio del 2007, aportando de sobre manera con un conjunto de buenas prácticas sobre objetivos de control de la seguridad de la información, compuesta por 11 dominios, 39 Objetivos de control y 133 controles.

- **ISO 27003 (en desarrollo)**

  Será un conjunto de recomendaciones y guías de implementación de un adecuado Sistema de Gestión de Seguridad de la Información basado en el modelo de Deming: Planear – Hacer – Controlar – Actuar y de las diferentes tareas que lo componen.

- **ISO 27004 (en desarrollo)**

  Tiene como objetivo determinar las métricas y técnicas de medición para determinar la eficacia de un SGSI y de los controles relacionados.

- **ISO 27005**

  Se enfoca en los lineamientos para una adecuada gestión de los riesgos en la seguridad de la información abarcando las normas ISO 27001 y 27002 bajo un enfoque de administración de riesgos.

Existen otras normas dentro de la serie de las ISO 27000 que se encuentran en fase de desarrollo y que verán la luz en los próximos años, referente a la seguridad en ambientes de redes y comunicación de datos, cyber-crimen, auditoria informática y seguridad de la información en centros hospitalarios y de sanidad.

2.4.2. La Gestión de la Seguridad de la Información basado en ISO 27002 (ISO 17799)

La Norma ISO 27002 está compuesta por dominios, objetivos de control y controles enfocados hacia el establecimiento de un adecuado Sistema de Gestión de la Seguridad de la Información (SGSI). Anteriormente dicha Norma tenía el nombre de ISO 17799, haciendo referencia a la norma británica BS 7799 que era un *Código de Práctica para la Administración de la Seguridad de la Información* y sobre la cual, se basó su contenido.

A través de la ISO 27002 se busca que la información sea confidencial, íntegra y disponible. Esto quiere decir, que la información solo puede ser accesible para las personas autorizadas; que la información debe ser exacta y confiable desde su ingreso hasta su presentación; y, que la información debe ser accesible vez que se requiera.

A continuación se hace un breve análisis de cada dominio dentro de la Norma:

1. **Política de Seguridad**

   La Alta Dirección debe establecer una política de seguridad de la información a nivel de toda la organización que demuestre su apoyo y compromiso hacia el control y salvaguarda del activo más importante de una organización: su información.

Para ello, debe existir un documento de seguridad de la información formalmente establecido por la alta gerencia; el mismo que debe ser continuamente revisado y actualizado; pero sobre todo, cumplido.

2. Organización de la Seguridad de la Información

En este dominio se abarca lo concerniente a la participación de la alta gerencia en la coordinación de los mecanismos que permitan implementar las políticas de seguridad de la información dentro de la organización.

Se debe determinar el rol de cada empleado dentro de la gestión de la seguridad de la información, así como sus responsabilidades y nivel de acceso a la información, ya sea como Propietarios o solo como Usuarios.

En este dominio también se abarca lo referente a contratos de servicios provistos por terceros; los acuerdos de confidencialidad; contacto con empresas amigas y con los entes reguladores para la aplicación de recomendaciones de seguridad; y, aspectos de seguridad con proveedores y clientes.

3. Gestión de Activos

Bajo este dominio se establecen los lineamientos sobre la administración y control de los activos físicos y lógicos, esto quiere decir, que debe existir un adecuado inventario de los equipos de computación y del software.

Se considera también como activos a las bases de datos, manuales técnicos y de usuario, instructivos de capacitación y de procedimientos; así como de los manuales de contingencias, equipos y muebles de oficina y utilitarios en general.

4. **Seguridad relacionada a los Recursos Humanos**

   En este dominio se establecen los lineamientos para la administración de la seguridad relacionada con el personal desde la fase de contratación hasta la fase de salida; considerando también entre otras cosas: la asignación de responsabilidades, la evaluación del desempeño y el manejo de conflictos.

5. **Seguridad Física y Ambiental**

   Bajo este dominio se encuentran las directrices para garantizar la seguridad física de los recursos tecnológicos, en especial de aquellos que son los más críticos dentro de la organización; como por ejemplo, los servidores, equipos de redes y comunicaciones, estaciones de trabajo de los altos ejecutivos, etc.

   Adicionalmente, se abarcan otros aspectos como el mantenimiento de los equipos computacionales, la entrada y salida de los recursos tecnológicos, la seguridad de las instalaciones, entre otras cosas.

6. **Gestión de las Comunicaciones y Operaciones**

   Este es uno de los dominios más amplios de la Norma y se abarca los principales aspectos dentro de la operatividad de los sistemas de información; las redes y comunicaciones; y, el comercio electrónico.

   Bajo este dominio se da mucho énfasis a la formalización de las políticas y procedimientos operativos dentro del área de TI, en los servicios prestados por terceros y en la segregación de funciones.

También se da mucha importancia al control del código fuente, en la verificación y validación de las copias de seguridad, la seguridad dentro de las redes, el intercambio de información con entidades externas y la auditoría de sistemas.

7. **Control de Acceso**

   En este dominio se dictan las directrices para el manejo adecuado de los Usuarios dentro de las aplicaciones, la gestión de contraseñas, los privilegios asignados, los controles en las computadoras conectadas a la red, control de computadores y dispositivos móviles, administración del dominio de red, administración de puertos de red, entre otras cosas relacionadas.

8. **Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información**

   Bajo este dominio se establecen los lineamientos más acertados dentro del ciclo de vida de los sistemas de información, la forma en que las aplicaciones deben mantener la seguridad durante el ingreso de datos, en el procesamiento y en la presentación de la información.

   Por otro lado, se abarca la seguridad de los archivos de las aplicaciones en producción y en desarrollo, la seguridad en los datos transmitidos a través de las redes, el manejo de software provisto por terceros, el control de cambios y el control de vulnerabilidades para su identificación y corrección.

9. **Gestión de Incidentes en la Seguridad de la Información**

   Este dominio a pesar de ser uno de los más pequeños, es bastante importante dentro de una correcta administración

de la seguridad, pues trata sobre la necesidad de que se realice un correcto registro de los incidentes o eventos de seguridad dentro de la organización; de tal forma, que se pueda analizar, estudiar su origen, medir el impacto y tomar los correctivos necesarios para que en la medida de lo posible, no vuelva a ocurrir.

10. **Gestión de la Continuidad del Negocio**

    Este es otro de los dominios más importantes dentro de la Norma, ya que enfatiza la necesidad de que existan procedimientos formalmente definidos para la prevención, mitigación y corrección de los eventos internos y externos potencialmente dañinos para la organización que pudiera poner en riesgo la operatividad de sus servicios.

11. **Cumplimiento**

    En dicho dominio se pone en claro la necesidad de que las organizaciones conozcan y apliquen la regulaciones gubernamentales vigentes, que se cumpla con las recomendaciones establecidas por los auditores externos y las entidades de control, así como también que se cumpla la legislación referente a propiedad intelectual.

2.5. Análisis de la interrelación entre los diversos estándares y mejores prácticas y su impacto en las COAC's

Como hemos visto hasta ahora, los diferentes estándares como COBIT, ITIL e ISO 27000 ofrecen una amplia gama de directrices respecto a la administración, ejecución y control de la Tecnología de Información.

Cada uno de dichos estándares se complementan de forma armoniosa dentro de los procesos de TI dando como resultado la construcción de un verdadero marco de gestión para las organizaciones de cualquier índole; y con mucha

más razón en las Entidades Financieras donde una adecuada gestión de TI puede significar el desarrollo o estancamiento de su crecimiento.

En el caso de COBIT, hay que resaltar que su enfoque es hacia el gobierno y administración de TI, agrupando las mejores prácticas de los diversos estándares existentes de gestión y control de TI, relacionándolo con los modelos de madurez, la gestión de riesgos y la generación de valor dentro de la organización.

Por otro lado, ITIL es un marco de trabajo enfocado hacia los servicios de TI, la forma en que deben ser planificados, administrados y ejecutados, detallándolos en una forma más amplia y especifica, complementando a las directrices de COBIT.

ISO 27000 por su parte se enfoca hacia la seguridad dentro de las diferentes directrices, planes, servicios y procesos de TI; de tal forma que se concentra no en la planificación, ni en la ejecución, sino en los controles que deben existir en cada una de las fases de gestión de TI y en la ejecución de los servicios derivados.

Por lo tanto, se podría decir que es posible combinar dichos estándares dentro de la gestión de TI en cualquier organización, obviamente realizando un estudio previo sobre los controles aplicables de acuerdo al tamaño y naturaleza de la organización.

A continuación se hace un pequeño mapeo de la interrelación de los tres estándares en forma general, esto quiere decir que se puede llegar a un nivel de detalle mucho mayor a nivel de los objetivos de control de bajo nivel en los tres estándares.

OBJETIVOS DE CONTROL COBIT	DOMINIOS DE ITIL	DOMINIOS ISO 27002 (ISO 17799)
PO1. Definir un plan estratégico de TI	Estrategia de Servicio	No es abarcado por ISO 27002
PO2. Definir la arquitectura de información	Diseño del Servicio Transición del Servicio	Gestión de Activos Gestión de las Comunicaciones y Operaciones Control de Acceso
PO3. Determinar la dirección tecnológica	Estrategia del Servicio Diseño del Servicio	Política de Seguridad Organización de la Seguridad de la Información Gestión de las Comunicaciones y Operaciones Control de Acceso Gestión de la Continuidad del Negocio
PO4. Definir los procesos, organización y relaciones de TI	Estrategia del Servicio Diseño del Servicio Transición del Servicio Operación del Servicio Mejora Continua del Servicio	Organización de la Seguridad de la Información Seguridad relacionada a los recursos humanos Cumplimiento Gestión de Activos Seguridad Física y Ambiental Gestión de las Comunicaciones y Operaciones
PO5. Administrar la inversión de TI	Estrategia del Servicio Transición del Servicio Operación del Servicio	Política de Seguridad Gestión de Incidentes de la Seguridad de la Información
PO6. Comunicación de la directrices gerenciales	Estrategia del Servicio Transición del Servicio Operación del Servicio	Política de Seguridad Organización de la Seguridad de la Información Gestión de Activos Seguridad relacionada a los recursos humanos Seguridad Física y Ambiental

		Gestión de las Comunicaciones y Operaciones Control de Acceso Mantenimiento de los Sistemas de Información Gestión de Incidentes de la Seguridad de la Información Cumplimiento
PO7. Administración del Recurso Humano de TI	Diseño del Servicio	Seguridad relacionada a los recursos humanos
PO8. Administrar con Calidad	Diseño del Servicio Transición del Servicio Mejora Continua del Servicio	Organización de la Seguridad de la Información Mantenimiento de los Sistemas de Información
PO9. Analizar y Administrar Riesgos	Estrategia del Servicio Diseño del Servicio Transición del Servicio Mejora Continua del Servicio	Política de Seguridad Gestión de Incidentes de la Seguridad de la Información Gestión de la Continuidad del Negocio
PO10. Administración de Proyectos	Diseño del Servicio Transición del Servicio Estrategia del Servicio	No es abarcado por ISO 27002
AI1. Identificación de soluciones automatizadas	Estrategia del Servicio Diseño del Servicio Transición del Servicio Operación del Servicio	Organización de la Seguridad de la Información Seguridad relacionada a los recursos humanos Gestión de las Comunicaciones y Operaciones Control de Acceso Mantenimiento de los Sistemas de Información
AI2. Adquisición y mantenimiento de Software de aplicación	Diseño del Servicio Transición del Servicio	Organización de la Seguridad de la Información Gestión de Activos

	Operación del Servicio	Gestión de las Comunicaciones y Operaciones Control de Acceso Mantenimiento de los Sistemas de Información Gestión de Incidentes de la Seguridad de la Información Cumplimiento
AI3. Adquisición y mantenimiento de la infraestructura tecnológica	Diseño del Servicio Transición del Servicio Operación del Servicio	Seguridad Física y Ambiental Gestión de las Comunicaciones y Operaciones Mantenimiento de los Sistemas de Información
AI4. Facilitar la Operación y el Uso	Diseño del Servicio Transición del Servicio Operación del Servicio	Gestión de las Comunicaciones y Operaciones Gestión de Incidentes de la Seguridad de la Información
AI5. Proveer Recursos de TI	Diseño del Servicio	Organización de la Seguridad de la Información Gestión de las Comunicaciones y Operaciones Mantenimiento de los Sistemas de Información
AI6. Administración de Cambios	Transición del Servicio Operación del Servicio Mejora Continua del Servicio	Gestión de las Comunicaciones y Operaciones Control de Acceso Mantenimiento de los Sistemas de Información
AI7. Instalar y Acreditar soluciones y cambios	Transición del Servicio Operación del Servicio Mejora Continua del Servicio	Organización de la Seguridad de la Información Seguridad relacionada a los recursos humanos Seguridad Física y Ambiental Gestión de las Comunicaciones y

		Operaciones Mantenimiento de los Sistemas de Información
DS1. Definir y administrar del nivel de servicio	Estrategia del Servicio Diseño del Servicio Transición del Servicio Operación del Servicio Mejora Continua del Servicio	Gestión de las Comunicaciones y Operaciones
DS2. Administrar servicios de terceros	Estrategia del Servicio Diseño del Servicio	Organización de la Seguridad de la Información Seguridad relacionada a los recursos humanos Gestión de las Comunicaciones y Operaciones Mantenimiento de los Sistemas de Información Cumplimiento
DS3. Administrar el desempeño y la capacidad	Diseño del Servicio Operación del Servicio Mejora Continua del Servicio	Gestión de las Comunicaciones y Operaciones
DS4. Asegurar el servicio continuo	Diseño del Servicio Operación del Servicio Mejora Continua del Servicio	Organización de la Seguridad de la Información Gestión de las Comunicaciones y Operaciones Gestión de la Continuidad del Negocio
DS5. Garantizar la seguridad de los sistemas	Diseño del Servicio Operación del Servicio	Política de Seguridad Organización de la Seguridad de la Información Seguridad relacionada a los recursos humanos Seguridad Física y Ambiental

		Gestión de las Comunicaciones y Operaciones Control de Acceso Mantenimiento de los Sistemas de Información Gestión de Incidentes de la Seguridad de la Información Cumplimiento
DS6. Identificación y asignación de costos	Estrategia del Servicio Diseño del Servicio Operación del Servicio	No es abarcado por ISO 27002
DS7. Educar y Entrenar a los Usuarios	Operación del Servicio	Seguridad relacionada a los recursos humanos
DS8. Administrar la Mesa de Servicio y los Incidentes	Operación del Servicio Mejora Continua del Servicio	Gestión de Incidentes de la Seguridad de la Información Gestión de la Continuidad del Negocio
DS9. Administración de la configuración	Estrategia del Servicio Transición del Servicio Operación del Servicio	Cumplimiento Gestión de Activos Gestión de las Comunicaciones y Operaciones Control de Acceso Mantenimiento de los Sistemas de Información
DS10. Administración de problemas e incidentes	Operación del Servicio Mejora Continua del Servicio	Gestión de Incidentes de la Seguridad de la Información Seguridad Física y Ambiental Gestión de las Comunicaciones y Operaciones Mantenimiento de los Sistemas de Información Cumplimiento
DS11. Administración de datos	Diseño del Servicio	Seguridad Física y Ambiental

	Operación del Servicio	Gestión de las Comunicaciones y Operaciones Mantenimiento de los Sistemas de Información Cumplimiento
DS12. Administración del Ambiente Físico	Diseño del Servicio Transición del Servicio Operación del Servicio	Organización de la Seguridad de la Información Seguridad Física y Ambiental
DS13. Administración de Operaciones	Diseño del Servicio Operación del Servicio	Seguridad Física y Ambiental Gestión de las Comunicaciones y Operaciones
ME1. Monitorear y Evaluar el desempeño de TI	Diseño del Servicio Operación del Servicio Mejora Continua del Servicio	Gestión de las Comunicaciones y Operaciones
ME2. Monitorear y Evaluar el Control Interno	No es abarcado por ITIL	Política de Seguridad Organización de la Seguridad de la Información Gestión de las Comunicaciones y Operaciones Cumplimiento
ME3. Asegurar el cumplimiento de requerimientos Externos	No es abarcado por ITIL	Organización de la Seguridad de la Información Cumplimiento
ME4. Proveer gobierno de TI	Estrategia del Servicio Diseño del Servicio Mejora Continua del Servicio	Política de Seguridad Organización de la Seguridad de la Información Gestión de las Comunicaciones y Operaciones

Tabla 2.3. Mapeo general de COBIT 4, ITIL V3 e ISO 27002 (ISO 17799:2005)

Como se puede notar en la tabla anterior, los tres estándares son perfectamente integrables y aplicables entre sí, de tal forma, que si se pudieran aplicar en forma armoniosa dentro de las Instituciones Financieras, en especial las COAC's, estamos frente a una óptima, eficiente, segura y confiable gestión de la tecnología de información.

Obviamente, la aplicación y combinación de dichos estándares implica fuertes inversiones en tecnología, tiempo, recursos y sobre todo una adecuada formalización de los procesos. En la medida de lo posible las COAC's deberán alinearse poco a poco a dichos estándares como parte del proceso de gestión del riesgo operativo, como veremos más adelante.

Capítulo 3.

La Administración del Riesgo Operativo dentro del Sistema Financiero Cooperativo

3.1. Estándares mundiales para el Control Interno y Administración del Riesgo en Entidades Financieras

3.1.1. El Control Interno basado en el COSO – ERM

3.1.1.1. COSO I

COSO Report o COSO I fue un informe sobre control interno elaborado en 1992 por el Committee of Sponsoring Organizations of the Treadway Commission de los EE.UU., con el objetivo fundamental de especificar un marco conceptual de control interno dentro de las organizaciones, capaz de integrar las diferentes políticas y lineamientos que la integran, permitiendo a la alta dirección mejorar sus sistemas de control interno.

Esto no quiere decir, que para lograr un adecuado control interno, sea suficiente cumplir al pie de la letra con las diferentes directrices establecidas en el COSO Report; sino que más bien, establecen un marco de control sobre las

cuales se fundamentan y se definen los lineamientos de control interno dependiendo del giro del negocio en cada organización.

Las organizaciones sobre todo financieras deben tener claro la importancia del Control Interno dentro de ellas como un conjunto de procesos, políticas y directrices establecidas por la alta dirección, aplicadas por todos los miembros de la organización, para obtener una ***seguridad razonable*** respecto al logro de los objetivos establecidos bajo las siguientes premisas:

- Eficacia y eficiencia en las operaciones.
- Confiabilidad de la información financiera.
- Cumplimiento con las leyes y regulaciones aplicables.

Nótese que lo que se logra con el Control Interno es una seguridad razonable respecto al logro de los objetivos establecidos. Por lo tanto, disponer de una estructura de control interno no garantiza un 100% de protección a nivel interno y externo frente a posibles fraudes, pérdidas financieras, información financiera adulterada, malversación de fondos, entre otros.

Por consiguiente, el control interno facilita pero no asegura que una empresa llegue a ser la más exitosa y confiable dentro de su industria. Debe haber un compromiso fuerte y trasparente hacia el control interno, desde la alta dirección hasta la persona que realiza la limpieza dentro de la organización.

Es por ello, que de acuerdo a COSO I, el Control Interno se basa en los siguientes componentes:

- **Ambiente de Control**

  Este componente se relaciona con la cultura organizacional de la Entidad, sobre todo, porque la alta dirección debe establecer normas de conducta adecuadas bajo principios éticos y honestos que sean adoptados por los miembros de la organización para que todas sus actividades sean desarrolladas bajo dichos principios. Sin un adecuado ambiente y compromiso hacia el control interno, los demás componentes no tendrían mayor efecto.

- **Evaluación del Riesgo**

  Las Entidades Financieras deben estar concientes que existen riesgos internos y externos a los cuales están expuestos. Una vez que se ha establecido dicha concientización que debe comenzar con la Alta Dirección, se deben identificar y evaluar cuales podrían ser las causas y sus potenciales eventos, comparándolos con los objetivos de la organización. En otras palabras, debe realizarse un mapeo de los objetivos de la Entidad Financiera frente a cada uno de los riesgos identificados y evaluar la forma en que dichos riesgos podrían ocasionar que no se cumplan los objetivos.

- **Actividades de Control**

  Una vez que se haya establecido un adecuado ambiente de control; se hayan establecido los objetivos empresariales y se haya realizado un adecuado análisis sobre los riesgos a los que la organización está expuesta, entonces se puede comenzar a delimitar las políticas y procedimientos de control para minimizar la ocurrencia y el posible impacto de los riesgos identificados.

Dichos controles no solamente tienen que ver con las áreas operativas o de bajo nivel en la organización, sino que involucra también [y con mucho mayor énfasis] a las áreas de alto nivel, incluida la gerencial y sino recordemos los casos de Enron (en EE.UU.) y Parmalat (en Italia) que dieron a lugar una crisis financiera en EE.UU., relacionado con las operaciones de cotización en la bolsa de valores y que ha dado a lugar incluso, para la producción de películas sobre dichos acontecimientos (Dick y Jane).

A este respecto, me permito hacer mención de la **Ley Sarbanes – Oxley** que fue emitida en el 2002 con la finalidad de monitorear a las empresas que cotizan en bolsa y sus filiales en el extranjero para evitar la adulteración o maquillaje de las acciones haciendo parecerlas atractivas a los inversionistas cuando su valor real no lo es.

Lo interesante de esta ley es que establece controles estrictos a la alta gerencia, al gerente financiero, al gerente de TI, auditor interno, auditores externos y organismos de control, ya que todos son co-responsables en la aplicación de los controles internos. Por lo tanto, las actividades de control deben existir a lo largo de todas las áreas de la organización.

- **Información y Comunicación**

  La Alta Dirección debe garantizar que exista una adecuada comunicación de las directrices políticas y procedimientos a nivel de toda la organización de tal manera que sea conocida por todos sus miembros y por otro lado, la información debe estar disponible para la correcta operación de sus actividades. Es por ello, que se

deben mantener sistemas de información confiables y seguros que permitan dicha fluidez de la información a los usuarios correctos.

- **Monitoreo**

  Se debe hacer un monitoreo y seguimiento de la aplicación de las políticas de control interno en cada una de las áreas de la organización, de tal forma, que se puedan encontrar en forma confiable y oportuna las deficiencias existentes para tomar las acciones correctivas e inmediatas.

  Para cada uno de dichos componentes, se desprenden una serie de actividades de control encaminados a implementar, monitorear y mejorar los objetivos de control.

3.1.1.2. El COSO – ERM o COSO II

En el 2004 el Committee of Sponsoring Organizations of the Treadway Commission formuló un nuevo marco de control mejorado del COSO, denominado ***COSO – ERM*** (Enterprise Risk Management) o también conocido como COSO II cuyo enfoque es el mismo que el de ***COSO Report*** pero basado en el riesgo.

El COSO – ERM toma los cinco componentes iniciales del COSO Report y les da un enfoque basado en la gestión de riesgos pero adicionalmente agrega 3 nuevos componentes.

Los componentes de COSO – ERM son los siguientes:

- **Ambiente Interno**

  Nótese que en el COSO Report (COSO I) el primer componente se denomina ***Ambiente de Control*** y comprendía la cultura organizacional y el establecimiento de principios a nivel de toda la organización; sin embargo desde el enfoque de riesgo, la Alta Dirección debe preocuparse por establecer el nivel de tolerancia permitido hacia el riesgo y que debe ser percibido por todos los miembros de la organización para que su desempeño y gestión se enfoque al riesgo bajo altos estándares de conducta y ética.

- **Establecimiento de Objetivos**

  Este es uno de los nuevos componentes que COSO – ERM incorpora, y en ella se destaca la necesidad de que la Alta Dirección defina los objetivos de la organización y defina los potenciales eventos que pudieran evitar que se cumplan bajo parámetros formales de análisis y considerando la tolerancia al riesgo aceptado por la Alta Dirección.

- **Identificación de Eventos**

  Este es otro componente nuevo y establece que la Alta Dirección debe realizar un análisis de cuáles son los eventos o acontecimientos internos o externos que afectan a la organización, tanto a nivel Interno y Externo, de tal forma, que se los pueda catalogar como riesgos o como oportunidades. Esto debe permitir que la gestión se adapte a dichos eventos para incorporar nuevas estrategias o nuevos controles bajo niveles de flexibilidad y redefinición de los objetivos. Esto significa que los objetivos no son estáticos sino

dinámicos y cambian de acuerdo al riesgo y las oportunidades.

- **Evaluación de Riesgos**

  Este es uno de los componentes más importantes dentro de la gestión del riesgo, ya que en él se establece que los riesgos deben ser analizados en forma detallada determinando cuales son las causas que pudieran provocarlo y su nivel de impacto para la organización, evaluándolos desde un punto de vista inherente y residual.

  Cabe anotar, que el riesgo inherente se refiere a aquel riesgo relacionado con la naturaleza del negocio y el riesgo residual se refiere a aquel tipo de riesgo que existe a pesar de haberse implementado los controles de prevención.

- **Respuesta al Riesgo**

  Este es otro nuevo componente, que en cambio establece que la Alta Dirección debe determinar qué va a hacer con los riesgos a los cuales está expuesta la organización. Esto quiere decir, que puede evitar, aceptar, reducir o compartir los riesgos

- **Actividades de Control**

  Este componente desde el punto de vista del riesgo, establece que la Alta Dirección debe determinar las políticas, procesos y procedimientos encaminados a tomar las acciones de respuesta al riesgo que previamente fueron analizadas y establecidas.

- **Información y Comunicación**

  Bajo este componente se resalta la necesidad de que exista información oportuna para una adecuada administración del riesgo, de tal forma que se pueda tomar decisiones oportunas y que la comunicación entre las diferentes áreas de la organización debe fluir de tal forma, que cada uno asuma sus responsabilidades bajo un ambiente de colaboración y prevención.

- **Supervisión**

  La Alta Dirección debe establecer mecanismos apropiados para determinar si los componentes anteriores se están cumpliendo cabalmente para que se puedan tomar los correctivos necesarios. Los Auditores Internos deben precautelar el cumplimiento de las actividades de control y recomendar a la alta dirección nuevos controles a ser incorporados como producto de las revisiones periódicas.

  Los Supervisores, en donde se incluye a la Superintendencia de Bancos, Auditores Externos y Calificadora de Riesgo tienen la obligación de realizar exámenes independientes sobre la gestión del riesgo dentro de la Entidad y realizar ellos sus propios análisis de riesgos para determinar si han sido cubiertos por la Entidad y de no ser así, recomendar su aplicación.

  Los Supervisores deben estar conscientes que el examen que realiza cada uno de ellos, debe ser independiente y no basarse únicamente en el informe proporcionado por otro supervisor porque eso podría provocar equivocaciones y errores de análisis o de criterios.

A continuación se muestra el cubo del COSO – ERM en donde se detallan sus objetivos y componentes:

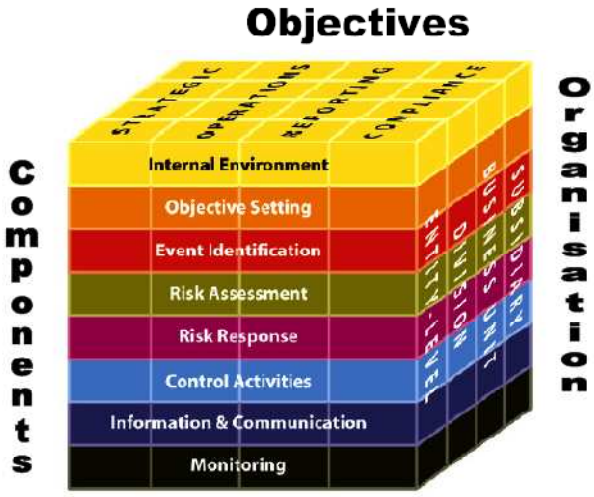


Figura 3.1. Cubo de COSO-ERM. (Fuente: http://www.itil.co.uk)

En general, podría resumirse los componentes de COSO-ERM de la siguiente manera:

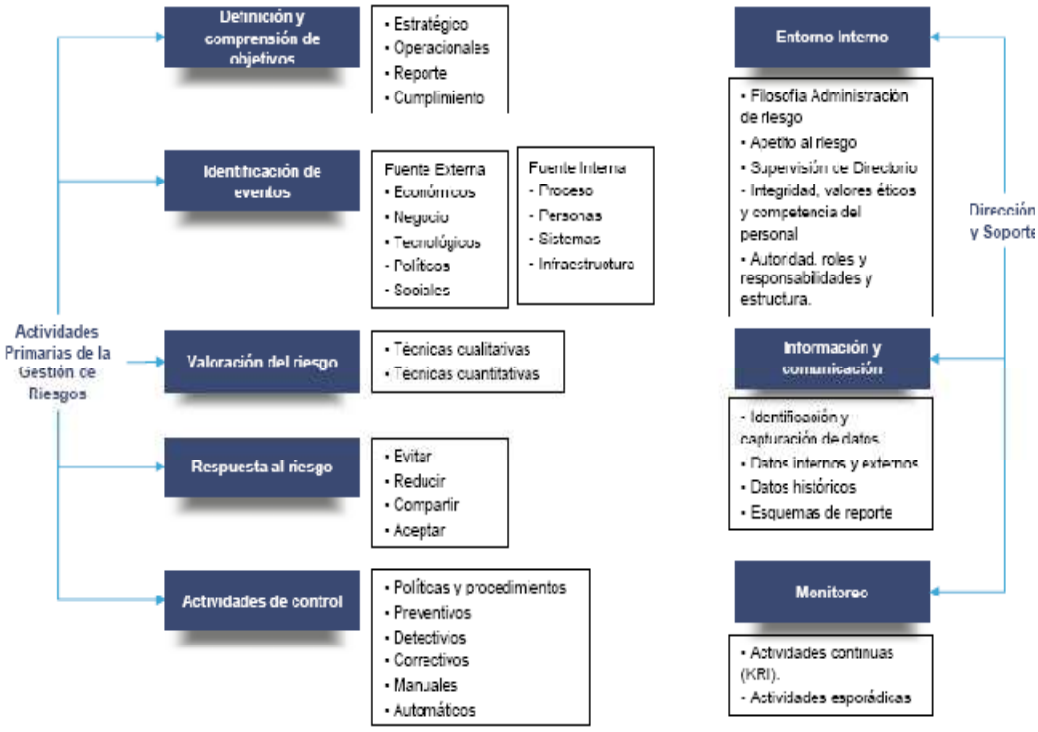


Figura 3.2. Resumen de los componentes de COSO-ERM (**Fuente:** Primer Congreso de Auditoría Interna - COSO II – ERM y el Papel del Auditor Interno / Rafael Ruano Diez

3.1.1.3. Las COAC's y el Control Interno

En el caso de las COAC's el control interno es parte fundamental dentro de sus procesos de negocio. Tal es así que inclusive la estructura jerárquica de dichas organizaciones hace especial énfasis en el control y monitoreo a nivel de toda la organización. Para ello, se encuentran claramente definidas funciones como el Consejo de Administración, el Consejo de Vigilancia, Auditoría Interna y la Unidad de Riesgos; las mismas que son las encargadas de velar por el cumplimiento de las directrices de control interno y las regulaciones exigidas por los Organismos de Control.

Adicionalmente a ello, hay que destacar la importante participación que tienen la Superintendencia de Bancos, el Servicio de Rentas Internas, las Calificadoras de Riesgo y los Auditores Externos, para la implementación de políticas de control interno en forma periódica a través de las revisiones y regulaciones que dichas entidades realizan.

3.1.2. Basilea II y su impacto en el Sistema Financiero

3.1.2.1. El Acuerdo de Basilea y sus Objetivos

El Comité de Basilea es un organismo internacional integrado por los directores de los bancos centrales de los países del primer mundo (Alemania, Bélgica, Canadá, EE.UU., Francia, Italia, Japón, Holanda, el Reino Unido, Suecia, Suiza, Luxemburgo y España), que ha emitido a través de los años, acuerdos y directrices sobre el funcionamiento y operación de las Instituciones Proveedoras de Servicios Financieros (**ENTIDADES FINANCIERAS**).

En 1988 se publicó el primer acuerdo de Basilea que se centraba en una serie de directrices respecto al capital mínimo que debía disponer una entidad bancaria frente a los riesgos que afrontaba.

Desde el 2007 hasta la actualidad, se encuentra vigente el Acuerdo de Basilea II que se centra en tres pilares fundamentales:

- **Mínimos requerimientos de capital**, que establece los requerimientos de capital basados en los riesgos de mercado, crédito y operacional.
- **Revisión de Supervisor**, que enfatiza la auditabilidad y transparencia de la entidad mediante la supervisión cualitativa del proceso interno del control de riesgos a través de los entes reguladores internos y externos.
- **Disciplina de Mercado**, que debe ser asumida por la entidad a través de la publicación de reportes al público respecto a su situación financiera y el control de riesgos realizado.

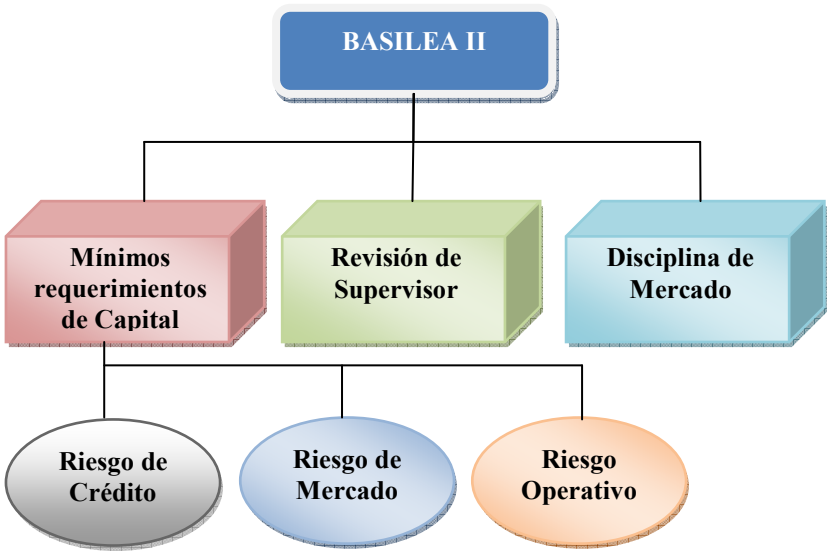


Figura 3.3. Pilares de Basilea 2

Como podemos ver, Basilea II centra sus objetivos en una adecuada regulación del sistema financiero a través de una correcta administración interna y mediante controles para los mercados financieros. Así mismo, busca que la gestión financiera de las entidades, se base en una adecuada identificación y administración de sus riesgos de manera íntegra, completa y sustentable bajo principios de honestidad y transparencia.

Lo interesante de esta norma es que incorpora dentro del análisis de los riesgos, al Riesgo Operacional, ya que anteriormente ya se había hecho énfasis en los riesgos de mercado, liquidez y crédito.

3.1.2.2. Basilea II y la Administración del Riesgo

De acuerdo a las directrices establecidas por el Acuerdo de Basilea II respecto a la administración del riesgo, se puede discernir lo siguiente:

- Las Entidades Financieras deben formalizar y adoptar un enfoque orientado a procesos respecto a la administración de los riesgos, la administración de la información y de sus procesos en conformidad con las normativas de la gestión corporativa.
- Las Entidades Financieras deben enmarcarse dentro de una estructura de gestión compleja y formal.
- Debe haber una adecuada integración de los sistemas involucrados en el manejo del crédito y las operaciones.
- Las soluciones de IT deben ser lo suficientemente flexibles para que el manejo de la información pueda

adaptarse a los cambios del sector financiero y de las nuevas regulaciones.

- No solo deben emprenderse proyectos de TI orientados al negocio sino también de proyectos que mejoren la estructura y los procesos de TI. Dichos proyectos deben ser auditables.
- La gestión administrativa debe ser capaz de encontrar el equilibrio entre la administración del riesgo y los beneficios obtenidos.

Como podemos ver, Basilea II da mucho énfasis a la administración del riesgo; aspecto que involucra de manera muy especial a la TI debido a que actualmente, como se ha enfatizado anteriormente, todas las Instituciones Financieras soportan sus operaciones en el uso de las TIC's y por tanto, las COAC's reguladas por la Superintendencia de Bancos y Seguros, deben adaptarse a dichos lineamientos.

3.1.2.3. Definición del Riesgo Operativo

De acuerdo al Instituto de Auditores Internos (The IIA) el riesgo se define como "la posibilidad de que ocurra un acontecimiento que tenga un impacto en el alcance de los objetivos". Por consiguiente, el riesgo se mide a través de determinar la probabilidad de que un evento que tiene un impacto negativo en la Entidad ocurra.

Aquello nos hace pensar, en que el riesgo es algo que está presente en las diversas actividades de una empresa sea cual sea su giro del negocio y más aún si ésta es una Entidad Financiera. Es por ello, que el Comité de Basilea define el **Riesgo Operativo** como: "la posibilidad de que se ocasionen pérdidas financieras por eventos derivados de fallas o

insuficiencias en los procesos, personas, tecnología de información y por eventos externos".

Cabe señalar, que el riesgo operativo incluye el **Riesgo Legal,** el cual se define como: "la posibilidad de que se presenten pérdidas o contingencias negativas como consecuencia de fallas en contratos y transacciones que pueden afectar el funcionamiento o la condición de una institución del sistema financiero, derivadas de error, dolo, negligencia o imprudencia en la concertación, instrumentación, formalización o ejecución de contratos y transacciones". El Riesgo Operativo no incluye al Riesgo Estratégico ni de Reputación.

Dentro de la administración del riesgo operacional, Basilea II establece la necesidad de disponer de un capital específico para su cobertura. Para calcular dicho capital se establecen tres métodos:

- **Método de Indicador Básico:** Establece que se debe cubrir el riesgo operacional con un capital equivalente a un porcentaje fijo de los ingresos brutos anuales medidos en los tres últimos años.
- **Método Estándar:** Se considera igualmente los ingresos brutos, pero el requerimiento de capital se calcula para cada línea de negocio.
- **Método de Medición Avanzada:** Cada Entidad utiliza sus propias estimaciones de de probabilidad interna para valorar razonablemente las pérdidas inesperadas.

3.1.2.4. Principios de Basilea II para la Administración del Riesgo Operativo

Basilea I planteó 25 principios fundamentales para una adecuada gestión financiera; los cuales, pueden ser leídos a través de la página Web de la Superintendencia de bancos y Seguros.

Basilea II toma como base dichos principios y agrega nuevos principios y directrices dentro de cada uno de sus tres pilares fundamentales.

Los principios relacionados con la administración del riesgo operativo formulados por Basilea II son los siguientes:

- **Compromiso de la Alta Dirección.** *El Consejo de Administración debe estar consciente de los principales aspectos de los riesgos operativos del banco, como una categoría de riesgo distinta que deben ser gestionados; y, debe aprobar y periódicamente revisar el marco de gestión del riesgo operativo del banco. El marco debe proporcionar a nivel de toda la empresa, una definición operacional de riesgo y establecer los principios de cómo el riesgo operacional debe ser identificado, evaluado, supervisado controlado y mitigado*.

- **Auditoría Interna Independiente y Competente.** *El Consejo de Administración deberá asegurar que el marco de administración del riesgo operativo está sujeto a una auditoría interna comprensiva y efectiva realizado por un equipo de trabajo independiente apropiadamente entrenado y competente. La función de Auditoría Interna no será directamente responsable de la administración del riesgo operativo.*

- **Marco de Gestión de Riesgos (MGR).** *La Alta Dirección será la responsable de implementar el marco de gestión del riesgo operativo aprobado por el Consejo de Administración. Dicho marco deberá ser implementado consistentemente a lo largo de toda la institución financiera y todos los niveles y áreas deberán comprender sus responsabilidades dentro de la administración del riesgo operacional. La Alta Dirección también tiene la responsabilidad de desarrollar las políticas, procesos procedimientos para la administración del riesgo operacional en todos los productos, actividades, procesos y sistemas de la entidad financiera.*

- **Identificación y Evaluación de Riesgos.** *Las Entidades Financieras deberán identificar y evaluar los riesgos inherentes en todos sus productos, actividades, procesos y sistemas. Además deberán asegurar que antes de introducir o adoptar nuevos productos, actividades, procesos y sistemas, los riesgos operacionales inherentes a ellos, serán sometidos a adecuados procedimientos de evaluación.*

- **Monitoreo del Riesgo Operacional.** *Las Entidades Financieras deberán implementar un proceso para monitorear regularmente los perfiles del riesgo operacional expuestos a pérdidas materiales. Aquello deberá ser reportado en forma oportuna a la Alta Dirección y al Consejo de Administración para una proactiva administración del riesgo operativo.*

- **Políticas, procesos y procedimientos formalmente establecidos.** *Las Entidades Financieras deberán*

establecer políticas, procesos y procedimientos para controlar o mitigar los riesgos operacionales materiales. Los bancos deberían revisar periódicamente sus riesgos y la limitación de las estrategias de control y deben ajustar sus perfiles de riesgo operativo mediante estrategias adecuadas, de acuerdo a sus necesidades y a sus perfiles de riesgo, en forma global.

- **Planes de Contingencia y de Continuidad del Negocio.** *Las Entidades Financieras deberán tener en sitio planes de contingencias y de continuidad del negocio para garantizar su capacidad de operación mínima y limitar las pérdidas en caso de una grave interrupción del negocio.*

- **Exigencias del Supervisor Bancario para un efectivo MGR.** *Los supervisores bancarios deberían exigir que todos los bancos, independientemente de su tamaño, dispongan de un Marco de Gestión de Riesgos (MGR) para identificar, evaluar, supervisar, controlar y mitigar los riesgos operativos materiales como parte de un enfoque global a la gestión del riesgo.*

- **Auditoría Independiente del Supervisor Bancario.** *Los supervisores bancarios deberán conducir directa o indirectamente, una evaluación independiente y regular de las políticas, procesos y procedimientos del banco, relacionados con el riesgo operacional. Los supervisores deberán asegurar que existen los mecanismos apropiados en la organización que les permita estar al tanto de los acontecimientos ocurridos en los bancos.*

- **Suficiente divulgación pública por parte de los bancos.** *Los bancos deberán realizar suficiente*

divulgación pública que permita a los diferentes participantes del mercado evaluar el enfoque de su gestión de riesgo.

ISACA a través del IT Governance Institute extrajo dichos principios de la gestión del riesgo operativo de Basilea II y los relacionó con los procesos de TI alineados con los cuatro dominios de COBIT.

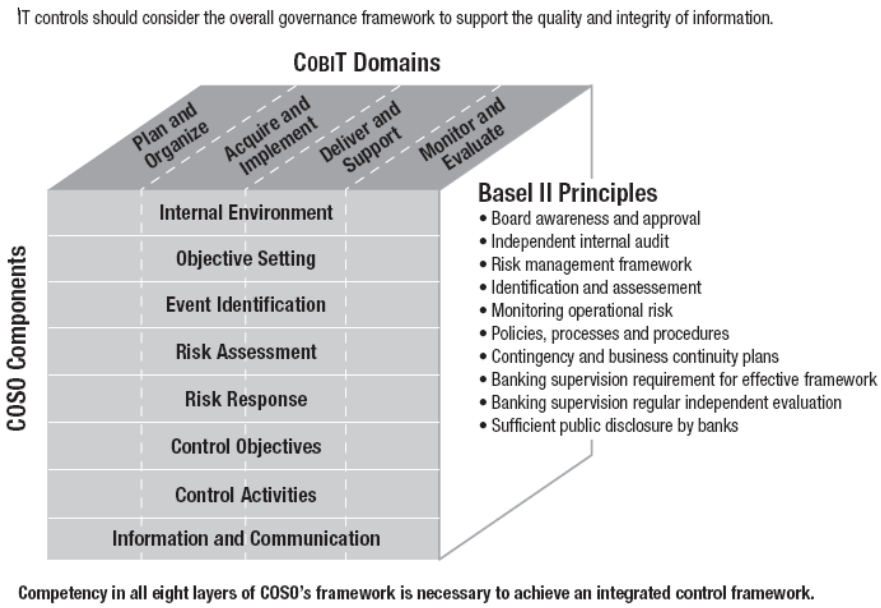


Figura 3.4. Alineación de COBIT, COSO-ERM y los 10 principios de Basilea II. (Fuente: **IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance**. / aut: IT Governance Institute. / http://www.isaca.org)

Para un mayor detalle de la forma en que se relacionan los 10 principios de Basilea II con COBIT 4, por favor remítase al **Apéndice 3. Principios de Basilea II mapeados con COBIT**.

Los lineamientos del comité de Basilea respecto a la administración del riesgo operativo están disponibles en dos documentos destacados:

- "Practicas adecuadas para la gestión y supervisión de los riesgos de operación".
- "El nuevo Acuerdo de Capital de Basilea": Metodologías de Medición de Capital por Riesgo de Operación.

En el caso de las COAC's, para muchas de ellas resulta muy complejo la aplicación de las directrices de Basilea II, debido fundamentalmente a que todavía están en proceso de formalización de sus procesos o en otros casos, se encuentran analizando paquetes de software para la ejecución de sus operaciones. Sin embargo, las COAC's bajo el control de la Superintendencia de Bancos, tienen el compromiso hasta Octubre del 2009 lograr dicho objetivo dentro de sus capacidades.

3.2. Leyes y regulaciones vigentes en el Ecuador para la regulación de las COAC's

3.2.1. La Norma 834 sobre Riesgo Operativo y su impacto en las COAC's

3.2.1.1. Historia y Alcance de la Norma 834

Dada la importancia que el Comité de Basilea le ha dado a la gestión del riesgo para el fortalecimiento de los Sistemas Financieros a nivel mundial, nuestro País ha hecho eco de dichas recomendaciones y tal es así, que a través de la Junta Bancaria el 22 de enero del 2004 emitió la Norma titulada "La Gestión Integral y Control de Riesgos" mediante la resolución No. JB-2004-631, en donde se enfatizaba la necesidad de que las Entidades Financieras de nuestro País

implementen un proceso de identificación, medición, control y monitoreo de los riesgos a los que se encuentran expuestos, incluido el riesgo operacional.

El 20 de Octubre del 2005, la Superintendencia de Bancos a través de la resolución Nº JB-2005-834 emitió la norma sobre ***Gestión del Riesgo Operativo***, que se encuentra en vigencia para todas las instituciones del sistema financiero que se encuentran bajo el control de la Superintendencia de Bancos y Seguros. De ahí en adelante, la Entidad controladora puso en marcha una serie de talleres y reuniones de trabajo con representantes de las diversas Instituciones Financieras para conocer sus comentarios y sugerencias respecto a la norma emitida y poder capacitar en detalle a quienes tendrían la responsabilidad de implementar la norma en cada una de sus entidades.

Para la elaboración de dicha norma se utilizó la literatura emitida por el Comité de Basilea respecto a las "Prácticas adecuadas para la gestión y supervisión de los riesgos de operación", así como la de "Administración de procesos" y "Administración del Recurso Humano"; mientras que para lo concerniente a la tecnología de información, se utilizó el marco de gestión de la seguridad de la información y de gobierno de TI de ISO 17799 y de COBIT respectivamente.

En la norma 834 de Riesgo Operativo se establecieron los lineamientos mínimos que deben seguir las entidades financieras para garantizar la continuidad del negocio frente a posibles riesgos a los que pudiera estar expuesta la entidad. Para ello, establece que se deben administrar en forma apropiada los procesos, personas, tecnología de información y los eventos externos.

Figura 3.5. Estructura del Riesgo Operativo. (Fuente: **Boletín de Asesoría Gerencial** / aut. Epiñeira, Sheldon y Asociados. http://www.pwc.com/ve/spa/pdf/aseger_200808.pdf)

3.2.1.2. La Administración de Procesos

Las Entidades controladas deben definir y formalizar de manera adecuada sus procesos basado en la planificación estratégica y las políticas establecidas. Para ello, se deben identificar, definir y administrar entre los procesos gobernantes o estratégicos, productivos u operativos; y, habilitantes o de apoyo.

Los procesos gobernantes se refieren a los procesos definidos por la alta dirección para la consecución de los objetivos institucionales y que abarcan la planificación estratégica, la estructura organizacional, la administración integral de riesgos, gerenciamiento de negocios, estrategias de mercado, etc.

Los procesos operativos, hacen referencia a los procesos relacionados con la operatividad y giro del negocio, como lo son los procesos relacionados a transacciones por ventanilla, de servicio al cliente, los procesos contables, procesos de tesorería, procesos de TI, etc.

Los procesos de soporte, abarcan la gestión documental y de archivo, de recursos humanos, soporte de TI, auditoría, control de calidad, adquisiciones, mantenimiento, entre otros.

Vale recalcar que la gestión se la hace por procesos no por departamentos, ya que un departamento podría realizar cualquiera de los tres tipos de procesos; como por ejemplo, los departamentos de TI realizan procesos de puesta en producción de aplicaciones y a su vez realizan procesos de soporte a Usuarios en el manejo de equipos computacionales.

Todas las políticas y controles que establezca la entidad, deben ser en base a los procesos que han sido previamente definidos. Es muy común que las organizaciones primero realizan sus políticas y objetivos de control y luego al identificar sus procesos, tratan de adaptar a sus procesos dentro de las políticas establecidas, ocasionando ineficiencia y controles débiles o inexistentes.

La administración de riesgos debe ser en base a dichos procesos a través de la identificación de las amenazas a las cuales están expuestos los procesos, las medidas preventivas de protección, las personas clave que intervienen dentro del proceso, las medidas de acción para enfrentar los eventos de riesgo y las medidas correctivas para mitigar la probabilidad de ocurrencia de dichos riesgos.

3.2.1.3. La Administración de las Personas

De Acuerdo a la Norma, las Entidades Financieras deben establecer adecuadas políticas, procesos y procedimientos para una correcta administración del capital humano en las diferentes etapas del personal dentro de la Entidad a saber: incorporación, permanencia y desvinculación. Aquello

permitirá a las Entidades administrar los riesgos asociados a las personas, tales como, negligencia, nepotismo, errores humanos, falta de personal, entre otros, que pudieran ocasionar deficiencias en la operatividad del negocio.

A continuación se especifica los procesos que comprende la administración de las personas:

- **Procesos de Incorporación,** que incluye el establecimiento de las necesidades a nivel de cada puesto o cargo; el reclutamiento adecuado, formal y estructurado; la selección basada en adecuados niveles de evaluación; la contratación bajo las leyes laborales vigentes; y, la inducción apropiada para un efectivo cumplimiento del puesto.

- **Procesos de Permanencia,** que permitan un óptimo y leal desempeño del personal en la realización de sus funciones y responsabilidades a través de un adecuado ambiente laboral, capacitación continua, evaluación y rendición de cuentas, un formal plan de carrera y estímulos suficientes que mantenga motivado al personal bajo una cultura organizacional claramente definida.

- **Procesos de Desvinculación,** que incluya un apropiado proceso de separación del personal bajo las leyes laborales vigentes que beneficie tanto al empleado saliente como a la Entidad.

Una correcta administración del capital humano involucra aspectos muy importantes de formalización de los diferentes procesos y actividades que la comprenden, ya que se debe establecer si la Entidad cuenta con el personal idóneo para la

realización de todos sus procesos, si el personal está motivado y comprometido con la Entidad, así como un compromiso por parte de la Entidad para brindar las condiciones laborales idóneas para su personal.

Además, involucra que la Entidad lleve un control del desempeño de su personal, de la capacitación y motivación requerida, de la evolución profesional y emocional que cada uno demuestra en la realización de sus responsabilidades.

3.2.1.4. La Administración de la Tecnología de Información

La Norma establece que se deben definir las políticas y procedimientos más adecuados para una correcta administración de la tecnología de información; la misma, que debe garantizar la correcta operatividad del negocio, la seguridad y confiabilidad de la información y una adecuada toma de decisiones.

Para ello, se deben establecer directrices sobre los cuales se encuadren los procesos de tecnología de información como los planes estratégicos, planes operacionales, políticas y procedimientos informáticos, manuales de funciones, niveles de autorización, etc.

Por otro lado, deben existir procedimientos claramente definidos respecto a la adquisición, asignación, uso y mantenimiento de los equipos computacionales para garantizar su correcto funcionamiento y salvaguardarlo frente a pérdidas o daños.

Además, las relaciones de soporte, mantenimiento y cualquier otro tipo de servicio provisto por terceros, deben tener los contratos de soporte formalmente establecidos bajo

criterios de cumplimiento y responsabilidad mutua, garantizándose que no existan vacíos legales y donde se establezcan políticas de confidencialidad para salvaguardar la información confidencial y de uso estratégico de la Entidad.

En lo que respecta a seguridad de la información, de acuerdo a la norma, deben existir políticas claras de seguridad informática, definir los responsables de la información, evaluar los riesgos, segregar adecuadamente las funciones, realizar auditorías informáticas, administrar el acceso a la información, mantener respaldos actualizados y confiables, manejo adecuado de versiones, entre otras cosas.

3.2.1.5. La Administración de los Eventos Externos

Las Entidades Financieras deben estar conscientes que están expuestas a diferentes eventos externos que pudiera ocasionarles pérdidas financieras derivadas de fallas en sus servicios, que incluso podría poner en riesgo la continuidad de sus operaciones con consecuencias muy graves, dada la sensibilidad de los clientes del Sistema Financiero.

Para ello, es necesario que se implementen medidas preventivas que consideren dichos eventos y su probabilidad de ocurrencia e impacto que minimicen su riesgo y que además se cuente con planes de contingencia y continuidad del negocio debidamente diseñados, formalizados y probados, bajo una política de mejora continua.

3.2.1.6. La Administración del Riesgo Legal

Como se mencionó anteriormente, el Riesgo Operativo incluye también al Riesgo Legal, el mismo que fue definido anteriormente, destacándose el objetivo que tiene de ***evitar o***

minimizar: las pérdidas financieras, una exposición altamente vulnerable de sus activos y un aumento inesperado de sus pasivos y contingentes; ***ocasionados por la inobservancia de***: las normativas legales vigentes y emitidas por los organismos de control; los dictámenes y resoluciones de los organismos de justicia; y, una adecuada prevención en la celebración de contratos y acuerdos con terceros.

La administración del Riesgo Legal cumple un papel muy importante dentro de la gestión del riesgo operativo como una herramienta de prevención dentro de los diferentes procesos y actividades que realizan las Entidades Financieras; tanto así, que para el Organismo de Control, el Riesgo Legal tiene una incidencia importante en todo el giro del negocio y en cada uno de los factores del riesgo operativo.

Se destacan los siguientes campos que incluye el riesgo legal:

- **Actos Societarios.-** Incluye los procesos jurídicos para la implementación de las decisiones del Consejo de Administración y de la Asamblea general de Socios para un adecuado desenvolvimiento societario de la Entidad. Se recomienda la existencia de un prosecretario para la generación y custodia de las Actas de Sesiones bajo estrictas normas de formalización y salvaguarda.

- **Gestión de Crédito.-** Tiene que ver con la formalización y correcta redacción de todos los documentos legales y sus procesos asociados que intervienen dentro de las diferentes etapas del

otorgamiento de los créditos desde la Solicitud hasta la Recuperación del Crédito.

- **Operaciones del giro financiero.-** Se relaciona a todos los aspectos legales concernientes a las diferentes operaciones de la Entidad diferentes a la gestión de crédito.

- **Actividades complementarias de las operaciones del giro financiero.-** Abarca a todas las particularidades jurídicas relacionadas con las actividades del negocio pero que no tienen relación con el giro del negocio.

- **Cumplimiento legal y normativo.-** Se relaciona con vigilar que la Entidad cumpla con todas las disposiciones legales y normativas de los organismos de Control y las leyes ecuatorianas y que se adapte en forma ágil y oportuna a nuevas resoluciones o disposiciones emitidas.

Por consiguiente basado en lo antes mencionado, para una efectiva administración del riesgo legal, es necesario que las COAC's trabajen en los siguientes aspectos:

- Disponer de un área legal para la administración de todos los aspectos jurídicos y societarios de la Entidad.
- Definir y formalizar políticas y procedimientos formales para la evaluación continua del riesgo legal por cada línea del negocio.

- Establecer y priorizar las normas y requerimientos legales que por incumplimiento pudiera ocasionar multas o sanciones a la Entidad, para que sean monitoreadas y controladas.
- Determinar las operaciones del negocio que por un incumplimiento legal o error operativo pudiera ocasionar una sanción o multa a la Entidad por parte de los organismos de Control.
- Establecer políticas y procedimientos para una adecuada formalización y revisión de TODOS los contratos bajo la supervisión del área legal de la Entidad.
- Que el Código de Conducta o de ética de la Entidad abarque los aspectos de compromiso o apego del personal a las normativas legales de la Entidad internas y externas.
- Disponer de bases de datos de carácter legal en donde se registre en forma histórica todas las normativas y resoluciones legales emitidas por los Organismos de Control, así como las acciones realizadas por parte de la Entidad para su cumplimiento.
- Crear una cultura organizacional orientada hacia un compromiso del personal en cumplir con las disposiciones legales emitidas por la Entidad y por parte de los Organismos de Control.

3.2.1.7. Las COAC's y la Norma 834

Muchas de las COAC's en un principio cuando se emitió la Norma 834 no fueron muy optimistas respecto a su aplicación dentro del sector cooperativo, por considerarla demasiado compleja considerando las operaciones dentro de la mayoría de las Cooperativas que son de tamaño pequeño,

en donde no cuentan con el personal y los recursos suficientes para aplicar las directrices que en ella se establecen.

Por ello, atendiendo la preocupación del sector cooperativo, la Superintendencia de Bancos ha realizado foros de capacitación, ha tenido reuniones con muchas cooperativas y ha flexibilizado el cumplimiento de la norma de acuerdo al entorno y posibilidades de cada Entidad. Incluso, para las COAC's el plazo de vencimiento para la aplicación de la norma es hasta el 31 de Octubre del 2009, mientras que para los bancos fue el 31 de Octubre del 2008.

En la actualidad, las COAC's están conscientes de la importancia y utilidad que tiene la Norma 834 dentro de sus operaciones, y han emprendido los proyectos de implementación de las directrices de la norma, incluso en algunos casos, agrupándose para colaborar entre ellas y a través de outsourcing de empresas de consultoría especializadas en el tema ya que reconocen que el incumplimiento de los lineamientos del riesgo operativo; además de las consecuencias anteriormente ya explicadas, podría ocasionar un alto *riesgo reputacional* para la Entidad.

En este sentido, se debe destacar que el ***riesgo reputacional*** es la posibilidad de que se forme una opinión pública negativa sobre el servicio bancario prestado; ocasionado por una falta de credibilidad o confianza hacia los clientes y de un mal servicio o falta de cobertura de las operaciones en el nicho objetivo de la Entidad; lo cual podría desencadenar en una disminución de las captaciones y posible cierre de la Entidad por falta de liquidez.

3.2.2. Entorno de Control de la Superintendencia de Bancos en el Sistema Financiero Cooperativo

3.2.2.1. Control de la Tecnología de Información

Como se ha visto a lo largo de esta Tesis, la Superintendencia de bancos ha tenido un papel muy importante dentro del control y medición de desempeño de las entidades financieras, en especial de las Cooperativas de Ahorro y Crédito.

Anualmente, la Superintendencia realiza auditorías de gestión a las entidades controladas, tratando de verificar el cumplimiento de las regulaciones establecidas. En la actualidad, aparte de las auditorias a los estados financieros, la Superintendencia de Bancos, realiza entre otras cosas, exámenes especiales a la gestión de crédito y cartera, los sistemas de información y el lavado de activos.

Las auditorías a los sistemas de información tienen la particularidad de ser muy exhaustivos ya que de ella depende el resto de los exámenes que se realizan a nivel financiero y operacional. Se evalúan las seguridades dentro de las aplicaciones, su eficiencia y confiabilidad.

En lo que respecta a las seguridades físicas, se revisa que existan las condiciones adecuadas para la operación de los equipos, que existan controles de acceso y que los equipos dentro del Core de Producción sean redundantes.

El manejo de las versiones es otra de las preocupaciones para los auditores de la Superintendencia de Bancos ya que se revisa que exista una adecuada segregación de funciones y procedimientos bien definidos para el manejo de versiones en las aplicaciones.

3.2.2.2. La Intendencia de Cooperativas

Las COAC's se han adaptado muy bien a dichos controles y han tratado de cumplir con dichas recomendaciones en forma oportuna y satisfactoria. Sin embargo, han existido ciertos requerimientos por parte de dichas entidades hacia la Superintendencia de Bancos, respecto a la supervisión dentro de dicho sector y la aplicación de Basilea II.

Entre dichos requerimientos estaba la creación de una Intendencia de Cooperativas de Ahorro y Crédito que realice la supervisión a dichas entidades de acuerdo a su realidad, ya que consideraban que eran comparadas al mismo nivel que los bancos privados.

Tal es así, que el 4 de Junio del 2008 se creó dicha Intendencia con el objetivo de que el control de las cooperativas ecuatorianas sea tomando en cuenta las mejores prácticas de control interno de acuerdo a su entorno, nivel de activos, número de socios, oficinas, etc.; y, en aspectos relativos a las operaciones de microcrédito, eje principal de las COAC's.

3.2.3. El apoyo en el control del riesgo operativo de los auditores externos y calificadoras de riesgo

Los Auditores Externos son firmas de especialistas en auditoria y análisis de estados financieros que dan una opinión, luego de cumplir con procedimientos de auditoría generalmente aceptados, sobre la razonabilidad de los Estados Financieros y sobre el cumplimiento a las regulaciones legales vigentes.

Las firmas de auditoría son un complemento a las revisiones efectuadas por la Superintendencia de Bancos e incorporan a las

auditorias de estados financieros, la revisión de los sistemas de información y el cumplimiento a las observaciones de la Superintendencia de Bancos. Entre las firmas más destacadas se encuentran:

- Price Waterhousecoopers Cía. Ltda.
- Deloitte & Touche Ecuador Cía. Ltda.
- Hansen - Holm Co. Cia. Ltda.
- Herrera Chang & Asoc.
- Kpmg Peat Marwick Cia. Ltda.
- Romero & Asociados Cia. Ltda.
- Salvador Aurea Cía. Ltda.
- Pkf & Co. Cía. Ltda.
- Bdo Stern Cía. Ltda.
- Consultores Moran Cedillo Cía. Ltda.

Por otro lado, se encuentran las calificadoras de riesgo que realizan revisiones especiales respecto al manejo de los riesgos de mercado y liquidez, de cartera y tecnológicos. Luego de dichas revisiones, emiten un informe en el que califican a una Entidad de acuerdo a una tabla que se muestra en el APÉNDICE 1.

3.2.4. Interrelación entre los diversos estándares de control y las regulaciones emitidas por parte de los Organismos de Control para las COAC's.

Como hemos podido observar, los lineamientos de control establecidos por COSO, Basilea II y la Norma 834 y que son aplicables para las COAC's y demás instituciones del Sistema Financiero, se basan e interrelacionan entre sí sobre tres pilares fundamentales:

El ***Gobierno Corporativo***,
La ***Administración del Riesgo*** y,

El ***Cumplimiento***

Figura 3.6. Pilares para una adecuada administración del riesgo operativo en las COAC's

Sí, esos tres rasgos o componentes son la base sobre la cual, se fundamentan los lineamientos de control interno hasta ahora estudiados y que al ser aplicados correctamente, deberían ser la clave para el logro de los objetivos institucionales, que junto a adecuadas estrategias de negocios, servicios e innovación competitiva; acompañado de un adecuado manejo de los costos, la cartera y las inversiones, deberían generar rentabilidad sostenible a las entidades del Sistema Financiero.

Pero sobre todo, no debemos olvidar que la mayor preocupación para la administración en las entidades financieras debe ser la salvaguarda de los recursos del público.

Las COAC's que se esfuercen en el cumplimiento de dichas normas antes mencionadas, lograrán tener una ventaja competitiva sobre las demás.

A continuación se muestra de manera general la forma en que dichas normas se relacionan entre sí:

PRINCIPIOS DE BASILEA II	COMPONENTES DE CONTROL INTERNO COSO - ERM	ASPECTOS DE CONTROL NORMA 834
1. Compromiso de la Alta Dirección	Ambiente Interno	**Art. 6:** Para una adecuada administración del riesgo operativo las instituciones controladas deberán cumplir las disposiciones del artículo 4 del presente capítulo y adicionalmente, deberán contar con códigos de ética y de conducta formalmente establecidos; con la supervisión del directorio u organismo que haga sus veces y de la alta gerencia; con una sólida cultura de control interno; con planes de contingencias y de continuidad del negocio debidamente probados; y, con la tecnología de información adecuada.
2. Auditoría Interna Independiente y Competente	Monitoreo / Seguimiento	**Art 12:** El esquema de administración del riesgo operativo de las instituciones controladas debe estar sujeto a una auditoría interna efectiva e integral, por parte de personal competente, debidamente capacitado y operativamente independiente. La función de auditoría interna coadyuva al mejoramiento de la efectividad de la administración de riesgos a través de una evaluación periódica, pero no es directamente responsable de la gestión del riesgo operativo.

3. Marco de Gestión de Riesgos (MGR).	Ambiente Interno	**Art. 4.2: Personas.-** Las instituciones controladas deben administrar el capital humano 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.
	Información y Comunicación	**Art. 4.3: 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.
4. Identificación y Evaluación de Riesgos	Establecimiento de Objetivos	**Art. 5:** En el marco de la administración integral de riesgos, establecido en la sección II "Administración de riesgos", del capítulo I "De la gestión integral y control de

	Identificación de Eventos Evaluación del Riesgo	riesgos", las instituciones controladas incluirán el proceso para administrar el riesgo operativo como un riesgo específico, el cual, si no es administrado adecuadamente puede afectar el logro de los objetivos de estabilidad a largo plazo y la continuidad del negocio. El diseño del proceso de administración de riesgo operativo deberá permitir a las instituciones controladas identificar, medir, controlar/mitigar y monitorear sus exposiciones a este riesgo al que se encuentran expuestas en el desarrollo de sus negocios y operaciones. Cada institución desarrollará sus propias técnicas o esquemas de administración, considerando su objeto social, tamaño, naturaleza, complejidad y demás características propias.
5. Monitoreo del Riesgo Operacional	Identificación de Eventos Evaluación de Riesgos Información y Comunicación	**Art. 6:** Para una adecuada administración del riesgo operativo las instituciones controladas deberán cumplir las disposiciones del artículo 4 del presente capítulo y adicionalmente, deberán contar con códigos de ética y de conducta formalmente establecidos; con la supervisión del directorio u organismo que haga sus veces y de la alta gerencia; con una sólida cultura de control interno; con planes de contingencias y de continuidad del negocio debidamente probados; y, con la tecnología de información adecuada.
6. Políticas, procesos y procedimientos formalmente establecidos.	Respuesta al Riesgo Ambiente Interno Actividades de Control	**Art. 4.1: Procesos.-** Con el objeto de garantizar la optimización de los recursos y la estandarización de las actividades, las instituciones controladas deben contar con

	Información y Comunicación	procesos definidos de conformidad con la estrategia y las políticas adoptadas…
7. Planes de Contingencia y de Continuidad del Negocio	Respuesta al Riesgo	**Art. 14:** Las instituciones controladas deben implementar planes de contingencia y de continuidad, a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción severa del negocio.
		Art. 15: Los planes de contingencia y de continuidad de los negocios deben comprender las previsiones para la reanudación y recuperación de las operaciones.
8. Exigencias del Supervisor Bancario para un efectivo MGR	Monitoreo	**Art. 21:** La Superintendencia de Bancos y Seguros podrá disponer la adopción de medidas adicionales a las previstas en el presente capítulo, con el propósito de atenuar la exposición al riesgo operativo que enfrenten las instituciones controladas. Adicionalmente, la Superintendencia de Bancos y Seguros podrá requerir a las instituciones controladas, la información que considere necesaria para una adecuada supervisión del riesgo operativo.
Auditoría Independiente del Supervisor Bancario	Monitoreo	**Art. 22:** En caso de incumplimiento de las disposiciones contenidas en este capítulo, la Superintendencia de Bancos y Seguros aplicará las sanciones correspondientes de conformidad con lo establecido en el capítulo I "Normas para la aplicación de sanciones pecuniarias", del título XVI ".
Suficiente divulgación pública por parte de los bancos	Ambiente Interno	**Art. 13:** Las instituciones controladas deben contar permanentemente con un

	Información y Comunicación	esquema organizado de reportes que permitan disponer de información suficiente y adecuada para gestionar el riesgo operativo en forma continua y oportuna.

Tabla 3.2. Interrelación entre BASILEA, COSO - ERM y La Norma 834.

3.3. Gestión del Riesgo Operativo en las COAC's

3.3.1. Lineamientos sobre la gestión del Riesgo Operativo

Como hemos visto anteriormente, el riesgo operativo involucra la administración de factores como los procesos, las personas, la tecnología y los eventos externos. Por ello, la administración del riesgo operativo involucra un análisis de todos los componentes de la organización a nivel interno y externo.

Las entidades controladas deben estar en la capacidad de implementar un sistema de administración del riesgo operativo que les posibilite la identificación, medición control y monitoreo de los riesgos asociados, bajo la premisa de fortalecer la solidez y seguridad de la Entidad con el objetivo de salvaguardar los recursos de sus depositantes.

Desde hace muchos años, con la aparición de las Normas Internacionales de Auditoria, las Normas Internacionales de Contabilidad (NEC en el Ecuador) y estándares como las SAS, el COSO y Basilea, las Instituciones Financieras y en particular las COAC's, han implementado controles dentro de sus procesos para la prevención de fraudes, evitar errores de ingreso y procesamiento de operaciones (transacciones bancarias), mejorar la eficiencia y garantizar la continuidad del negocio.

Sin embargo, dichas directrices de control eran vistas como recomendaciones y buenas prácticas, más no como un requerimiento de cumplimiento, por lo que a través de la formalización de dichos

controles dentro de la norma de riesgo operacional, se busca su cumplimiento de facto dentro de las entidades controladas; más aún ahora en donde han crecido el volumen de las operaciones y montos de captaciones y cartera que manejan las entidades financieras; la aparición de nuevas tecnologías, productos y servicios financieros; el crecimiento del uso del e-Commerce y el e-Business; y la globalización.

En general, para una adecuada gestión de riesgos es necesario que se cumplan con los siguientes lineamientos:

- Establecer un adecuado ambiente de administración de Riesgos.
- Realizar una gestión proactiva de los riesgos.
- Asumir e implementar las observaciones y recomendaciones de las entidades de control.
- Transparencia de la información financiera y de la gestión de riesgos realizada.

Ya en la práctica, cada Entidad de acuerdo a su tamaño, naturaleza y capacidades podrá implementar encuestas de autoevaluación, indicadores, mapas de riesgo, balance scorecards, aplicaciones especializadas, bases de datos, hojas de cálculo, entre otros tipos de herramientas.

3.3.2. Gestión de Riesgos en Entidades controladas

La administración del riesgo en las Entidades controladas nace desde el directorio o del consejo de administración según sea el caso, estableciendo las estrategias y la infraestructura de vigilancia para la administración y mitigación del riesgo en base a las recomendaciones del Comité de Administración Integral de Riesgos.

La Unidad de Auditoría Interna debe revisar y supervisar la implementación de dichas estrategias e infraestructura, recomendar los

cambios necesarios y vigilar su cumplimiento, el auditor interno es un "asesor", no un crítico, pero tampoco un implementador. Debe mantener la independencia funcional.

La Gerencia General es la encargada de armar la infraestructura y poner en funcionamiento toda la "maquinaria" necesaria para la adecuada gestión del riesgo operativo. Para ello, se valdrá de la Unidad de Riesgos que será la encargada de implementar los controles, vigilar su cumplimiento e informar sobre los resultados obtenidos.

La Unidad de Riesgos es la responsable de identificar y evaluar los riesgos de acuerdo a los procesos, productos, servicios, actividades y sistemas de información. Debe identificar el grado de exposición y las pérdidas esperadas. Establecer las políticas, procesos y procedimientos para la mitigación de los riesgos; y, diseñar, probar y mejorar el plan de continuidad del negocio.

La Norma 834 para una adecuada gestión del riesgo operativo recomienda que se cumpla con sus directrices respecto a la administración de los procesos, personas tecnología de información y eventos externos, agrupando sus procesos por línea de negocio, identificando para cada una de éstas sus eventos de riesgo, las mismas que están agrupadas de la siguiente manera: Fraude Interno, Fraude Externo, Prácticas laborales y seguridad del ambiente de trabajo, practicas relacionadas con los clientes, productos y negocios, daños a los activos físicos, fallas de tecnología de información; y, deficiencias en la ejecución de procesos, operaciones y relaciones con proveedores y terceros.

La metodología que utilice cada Entidad para la evaluación de sus riesgos queda a su criterio y bajo sus posibilidades y necesidades, lo importantes es que la Alta Dirección cuente con la información necesaria para la toma de decisiones oportuna de tal forma que pueda

decidir si lo asimila, lo enfrenta, lo transfiere o lo comparte a través de acciones concretas y eficaces. Para ello, se requiere que las Entidades registren sus eventos de riesgo cada vez que estos ocurran y dispongan de bases de datos estructuradas y de calidad con dicha información para evaluar la frecuencia de ocurrencia y las pérdidas esperadas mediante informes gerenciales de alto valor que además consideren la efectividad de los controles a través de indicadores de gestión.

Los Organismos de Control, Auditores Externos y Calificadora de Riesgo por su parte, deberá verificar que cada instancia cumpla con sus responsabilidades respecto a la administración del riesgo y exista una estructura fuerte para la adecuada consecución de los objetivos establecidos para dicho fin. Para ello, se deberá evaluar los manuales, políticas, procedimientos y actas de sesión de los distintos comités; pero sobre todo verificar que estén formalmente aprobadas.

3.3.3. El papel del Comité de Administración Integral de Riesgos y de la Unidad de Riesgos

El Comité de Administración Integral de Riesgos cumple un papel fundamental dentro de las COAC's ya que a través de dicho comité se definen las estrategias y lineamientos de gestión de riesgos dentro de la Entidad y que luego será aprobado por el Consejo de Administración.

Dentro de sus integrantes por lo general se encuentran el Gerente General, el Gerente o Jefe de Riesgos, el Gerente o Jefe de Crédito, el Gerente Financiero y el Gerente de Operaciones. Dependiendo de la estructura, necesidades y tamaño de la organización dicha estructura podría cambiar.

Entre los factores de riesgo que el Comité de Administración Integral de Riesgos evalúa, también se encuentran los tecnológicos; lo cual, significa que debe existir la participación del Gerente o Jefe de

Sistemas dentro de los análisis de riesgos de la organización para garantizar que se encuentren alineados correctamente hacia un ámbito completo e integral.

La responsabilidad de dicho Comité también involucra la definición y formalización de los diferentes planes de contingencia departamentales hasta el plan de continuidad del negocio organizacional.

Por otro lado, existe otra instancia de control como la Unidad de Riesgos que es la encargada, en base a las estrategias y lineamientos definidos por el Consejo de Administración Integral de Riesgos, de diseñar las políticas y los procesos de administración del riesgo operativo.

A su vez, esta Unidad es la encargada de monitorear y evaluar los cambios significativos del grado de exposición a los riesgos a la que se encuentran los procesos, las personas, tecnología y eventos externos. La Unidad de Riesgos, además es la responsable de analizar las políticas de seguridad de la información establecidas por el área de TI.

Respecto a los planes de contingencia y de continuidad del negocio, dicha Unidad de Riesgos, debe participar en su elaboración recomendando los lineamientos y medidas más adecuadas, monitorear que se apliquen y recomendar las personas responsables de cada tarea, de acuerdo a idoneidad y capacidad.

Capítulo 4.

Establecimiento de un Marco de Control para la implementación de una adecuada Administración del Riesgo Tecnológico en las COAC's

4.1. La Administración del Riesgo Tecnológico en las COAC's

4.1.1. La Información frente al Riesgo Tecnológico

En la actualidad la tecnología de información está presente en casi la totalidad de los negocios y organizaciones tanto públicas como privadas en todo el mundo. Dicha automatización de los procesos ha permitido que las organizaciones puedan desarrollarse de forma acelerada en el entorno competitivo y globalizado del mundo de hoy. Sin embargo, aquello supone también que las organizaciones cuyos procesos se encuentran automatizados a través de la tecnología de información, desarrollen una dependencia hacia ella que a la larga sin una adecuada administración del riesgo tecnológico podría traer consecuencias muy negativas.

Es por ello, que uno de los factores del riesgo operativo es la tecnología de información; ya que en la medida en que una organización dependa de la tecnología de información, los riesgos asociados a ella serán transferidos a la organización. Por consiguiente, se debe identificar los características de la información que deseamos

proteger y que son de alto impacto para la organización su falta de aplicación.

COBIT identifica siete características de la información sobre las cuales se debe basar el análisis del riesgo. Ellas son: Efectividad, Eficiencia, Confidencialidad, Integridad, Disponibilidad, Cumplimiento y Confiabilidad. Esto quiere decir, que se recomienda que todas las medidas preventivas y correctivas de control hacia la tecnología de información, deben buscar garantizar dichas características y mitigar los riesgos asociados a cada una de ellas. En términos generales deberá considerarse lo siguiente respecto a:

- **Efectividad:** Se debe garantizar que la información sea relevante, oportuna y utilizable para cada línea de negocio. Por ejemplo, garantizar que el área de cartera pueda disponer de reportes de cartera vencida con información detallada del cliente en forma oportuna.
- **Eficiencia:** La información debe estar disponible con un eficiente uso de los recursos. Por ejemplo, garantizar que las áreas de ventanillas dispongan de un suficiente y prioritario ancho de banda para las transacciones frente a los accesos comunes a Internet de otras áreas.
- **Confidencialidad:** Garantizar que la información sea accedida por quienes tienen la autorización para ello. Por ejemplo, disponer de accesos bajo roles y perfiles para los Usuarios y garantizar el sigilo bancario.
- **Integridad:** La información no puede ser alterada o presentar errores. Por ejemplo, la acreditación de intereses y los saldos de las cuentas de ahorros deben ser precisas y no propensa a errores.
- **Disponibilidad:** La información debe estar disponible en todo momento para garantizar la continua operatividad del negocio. Por ejemplo: disponer de un centro de cómputo alterno en una Agencia o sucursal en otra ciudad fuera de la oficina Matriz.

- **Cumplimiento:** La información debe cumplir con las leyes vigentes y estar disponible para los Organismos de Control cuando estos lo requieran. Por ejemplo: Cumplir con la normativa de transparencia de la Información dispuesta por la Superintendencia de Bancos y Seguros.
- **Confiabilidad:** La información debe ser precisa y confiable para la toma de decisiones. Por ejemplo: Información generada para la gerencia sobre los saldos de tesorería e inversiones vigentes, históricos y proyectados para la planificación de las colocaciones a futuro.

4.1.2. Lineamientos para una eficaz Administración del Riesgo Tecnológico en las COAC's

La gestión de los riesgos de TI no es una responsabilidad que recae solamente sobre el Jefe de Sistemas, sino que es una responsabilidad que abarca desde la alta dirección hasta los niveles operativos de la Entidad. De nada servirá que exista un avanzado sistema para la administración de perfiles y roles mientras los Usuarios se prestan y comparten las contraseñas. Es por ello, que además de las políticas y procedimientos de control, es necesario una concientización de los Usuarios y responsables de la administración de los recursos de TI acompañado de capacitaciones continuas.

Así mismo, la Superintendencia de Bancos y Seguros a través de sus auditores en las revisiones anuales de TI en las Entidades Financieras, han recomendado que se formalice un Comité que evalúe en forma continua la gestión de TI, el mismo que tomará el nombre de Comité de Informática que podría estar conformado por: el Jefe de Sistemas, el Auditor de Sistemas, el Oficial de Seguridad y el Jefe de Operaciones.

En general, para una adecuada administración de los riesgos de TI en las COAC's se recomienda lo siguiente:

1. **Definir una estrategia corporativa para administrar el riesgo tecnológico**, a través de una política de seguridad formalmente establecida alineada con el plan estratégico del negocio. La estrategia de administración del riesgo de TI deberá considerar:
    - Una estrategia de Gobierno de Tecnología de Información.
    - Una estrategia de seguridad de la información.
    - Una estrategia de alta disponibilidad
    - Una estrategia de redes y comunicaciones
    - Una estrategia de análisis y mitigación de riesgos

2. **Crear una Cultura Organizacional enfocada al Riesgo Tecnológico**, que concientice a todos los Usuarios de los recursos tecnológicos que tienen la responsabilidad de vigilar y garantizar la protección de dichos recursos; además de prevenir cualquier tipo de evento negativo y comunicar a quien corresponda, sobre posibles amenazas y vulnerabilidades.

3. **Organización del Área de TI**, lo que incluye definir formalmente los perfiles y realizar una descripción de cargos detallada para cada puesto del área de TI, debidamente aprobado por el Consejo de Administración y conocido cabalmente por cada miembro del área de TI.0

4. **Definición de los procesos de TI,** que formalice las diferentes actividades, procesos, procedimientos que realiza el área de TI de tal manera que cada uno de sus miembros conozca la forma en que debe realizar sus funciones y responsabilidades, ya que sobre ello se realizarán las evaluaciones del personal. Esto permite además, que no exista dependencias funcionales que ponga en riesgo la continuidad de los procesos ante la falta de algún funcionario del área de TI. Dentro de esta etapa se debe

diseñar un mapa de integración de los procesos de la organización versus los procesos de TI.

5. **Analizar y evaluar los riesgos de tecnología y su impacto sobre el negocio,** lo que incluye realizar una definición detallada de todos los posibles eventos negativos que pudieran ocasionar un riesgo a la tecnología de información, sus posibles causas, su probabilidad de ocurrencia, su impacto, los procesos relacionados a ellos, los responsables, los controles preventivos y las acciones correctivas a tomarse.

   Dentro de este análisis debe considerarse la información interna, externa, estudios y estadísticas sobre eventos negativos de TI, evaluar diversos escenarios, considerar el ambiente del negocio y comportamiento del mercado, regulaciones legales y controles internos.

6. **Diseñar e Implementar un Plan de Acción continuo**, que en base al análisis de riesgos permita implementar los controles y medidas preventivas para minimizar o asumir el riesgo de TI. Dicho Plan debe ser flexible y adaptable a las necesidades de la organización y debe ser reformulado de manera periódica de acuerdo a una política de mejora continua. El Plan debe abarcar, por cada proceso de TI, las medidas preventivas, correctivas y de recuperación frente a cada escenario y evento negativo a los que puede estar expuesta la TI de la Entidad.

7. **Monitorear y alimentar una base de datos de Eventos,** a través de un trabajo continuo entre el Oficial de Seguridad y Auditoría Interna para por un lado, monitorear el cumplimiento del plan de acción y por otro lado auditar y recomendar las mejoras pertinentes para la gestión del riesgo de TI.

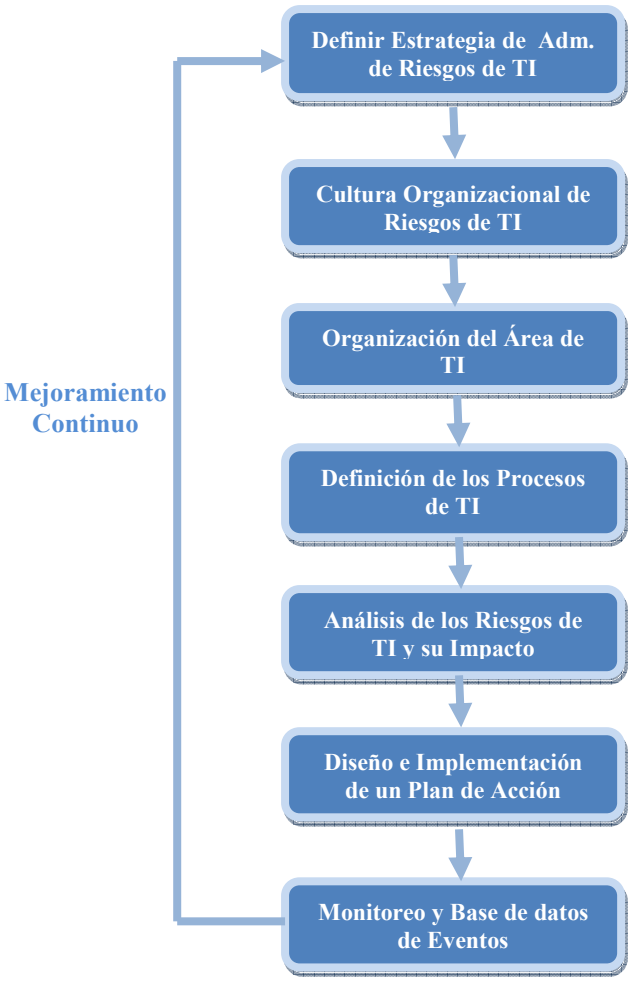


Figura 4.1. Flujo de procesos para la administración de riesgos de TI

4.2. Planificación y Administración de la Tecnología de Información

4.2.1. Introducción

Todas las organizaciones exitosas sin importar el giro o naturaleza del negocio, están conscientes de que antes de poder emprender sus operaciones, necesitan establecer sus objetivos y metas de manera clara y específica, de tal forma, que sepan el rumbo que deben seguir y cuál es el horizonte mínimo que deben alcanzar.

Dicho horizonte se convierte en un factor de medición al momento de evaluar los resultados obtenidos. Sin embargo, no basta con solo determinar hasta dónde quiere llegar la organización para que

aquello se dé; es necesario además, establecer las estrategias necesarias para lograr dicho horizonte, es decir, el cómo lograrlo.

Es por ello, que es muy común que cada año, en las organizaciones, se diseñen planes estratégicos empresariales en donde se plantean: los objetivos, las metas, recursos necesarios, indicadores de medición y desempeño, estrategias de marketing, entre otros. Sin embargo, en muchas ocasiones la gestión tecnológica no es considerada dentro de dicha planeación estratégica y si se lo hace, se limita a un presupuesto de adquisición de equipos de computación.

Dicha realidad, no escapa de lo que sucede en algunas COAC's, sobre todo en las medianas y pequeñas, en donde a pesar que poseen planes empresariales, no disponen de una adecuada planificación tecnológica, acorde a sus proyecciones de crecimiento, y su capacidad adquisitiva.

A continuación, dentro de la presente sección, se establecen algunos lineamientos dentro de la planificación de tecnología de información que deben tomar en cuenta las COAC's dentro de su gestión de riesgos.

4.2.2. Evaluación de Riesgos de TI

El Comité de Riesgos debe evaluar en forma minuciosa los riesgos a los que está expuesta la organización, de tal manera, que se implementen los controles necesarios para mitigarlos.

La Superintendencia de Bancos y Seguros recomienda, basado en los lineamientos del Comité de Basilea, que dentro de dicha evaluación se debe considerar por lo menos los riesgos asociados a los siguientes tipos de eventos:

- Fraudes Internos
- Fraudes Externos

- Prácticas de Empleo y Seguridad del Ambiente de Trabajo
- Prácticas relacionadas con Clientes, Productos y el Negocio
- Daños a los Activos Físicos
- Interrupción del negocio y fallas en los Sistemas
- Deficiencias en la Ejecución de Procesos, en el procesamiento de Operaciones y en las relaciones con proveedores y Otros Externos.

Una vez, evaluado, los tipos de eventos, sus riesgos asociados, tipo de factor (endógeno o exógeno), la probabilidad de ocurrencia y las acciones a tomarse para mitigar dichos riesgos, debe realizarse un informe que detalle dicho análisis y que debe ser conocido por el Consejo de Administración, el Comité de Auditoría y la Gerencia General para que la planificación estratégica, las operaciones y las revisiones de control y auditoría se basen en dicho análisis de riesgos.

La Planificación estratégica de TI debe basarse en el análisis de riesgos de la organización; sí, de toda la organización y no solamente los riesgos asociados a TI. De esa manera, la gestión del riesgo será administrado en forma oportuna, completa y eficaz con el soporte del área de TI.

En forma puntual, al evaluarse los riesgos de TI debe considerarse por lo menos lo siguientes eventos:

- Fallas en el Software
- Fallas en el Hardware
- Fallas en las Redes y Comunicaciones
- Fallas en los Servicios WEB
- Ataques Internos
- Ataques Externos
- Cortes de Energía
- Incendios

- Terremotos
- Inundaciones
- Terrorismo
- Corrida de retiro de depósitos
- Fallas en el envío de información a Organismos de Control
- Mal Uso de Equipos por parte de los Usuarios
- Virus y diversos tipos de malware, entre otros.

4.2.3. El Plan Estratégico de Tecnología de Información

Consiste en determinar con un horizonte de por lo menos dos años, los proyectos, adquisiciones e inversiones de tecnología de información que serán necesarias para cumplir con los objetivos del negocio de acuerdo a la planificación estratégica definida por la alta dirección. Esto quiere decir que el plan estratégico de TI debe estar plenamente alineado con el de la organización y no en forma independiente.

Respecto a aquello, cabe señalar que en la práctica muchos planes estratégicos de TI son elaborados sin tomar en cuenta el plan estratégico empresarial, generando inconsistencias respecto a los planes de TI frente a los planes de la alta dirección.

El Plan estratégico de TI debe abarcar las necesidades de cada una de las áreas de la organización y a su vez, debe considerar los nuevos productos o servicios que la organización ha planificado implementar dentro del horizonte considerado (mínimo dos años).

En este punto, hay que destacar que una vez cubierta las necesidades del negocio, se debe evaluar los proyectos y adquisiciones necesarios para mitigar los riesgos a los que está expuesta la organización, con el objetivo de que la administración del riesgo sea plenamente cubierta.

Finalmente, se debe determinar en base a la estructura tecnológica actual, los recursos necesarios para su adecuada administración y para el cumplimiento con las leyes y regulaciones vigentes.

Para el caso de las COAC's, un Plan Estratégico de TI podría tener la siguiente estructura:

- Misión y Visión de la Entidad
- Misión y Visión del área de TI
- Objetivos y metas de la Entidad
- Objetivos y Metas del área de TI
- Entorno Interno y Externo de TI en la Entidad
- Detalle de los recursos tecnológicos disponibles por la Entidad
- Resumen de Proyectos planificados de TI
- Análisis de factibilidad y planeación detallada de los proyectos y servicios de Hardware
- Análisis de factibilidad y planeación detallada de los proyectos y servicios de Software
- Análisis de factibilidad y planeación detallada de los proyectos y servicios de Redes y Comunicaciones
- Análisis de factibilidad y planeación detallada de los proyectos y servicios de seguridad y continuidad del negocio
- Análisis de factibilidad y planeación detallada de otros proyectos y servicios de tecnología (otros aspectos tecnológicos asignados al área de TI)
- Planificación de Capacitación del personal de TI
- Renovación de Contratos por Servicios outsourcing
- Adquisición y Renovación de Licencias de Software
- Presupuesto de inversiones en TI
- Cronograma preliminar de los proyectos de TI

Esta estructura es una recomendación de los posibles aspectos que podrían incluirse dentro de un Plan Estratégico de TI, pero obviamente dependerá de la Entidad la estructura definitiva a seguirse. El Plan Estratégico debe ser aprobado formalmente por el Consejo de Administración.

4.2.4. El Plan Anual de Tecnología de Información

El Plan Anual de TI, también denominado Plan Operativo Anual o Plan Maestro Anual, es un plan de acción para llevar a cabo la planeación estratégica de manera efectiva. Esto quiere decir, que en dicho plan se detallan los proyectos, adquisiciones, tareas, presupuestos, cronogramas, capacitación y demás aspectos relacionados con la gestión de TI, necesarios para cumplir con lo planificado durante el año en curso.

Es muy importante que dicho plan sea completo y flexible respecto a los proyectos de TI; de tal manera, que en caso de que los proyectos planificados sean redefinidos en cuanto a su estructura, plazos y tiempos límites, se puedan realizar de manera exitosa. El Plan Anual no es una camisa de fuerza, es una herramienta muy importante para la correcta gestión de los proyectos y recursos de TI y sobre todo para garantizar el control y cumplimiento de lo planificado por el área de TI.

El Plan Anual deberá contemplar por lo menos lo siguiente:

- Objetivos y Metas de TI para el año en curso.
- Proyectos y adquisiciones de Hardware
- Proyectos y adquisiciones de Software
- Proyectos y adquisiciones de Redes y Comunicaciones
- Proyectos y adquisiciones de Seguridad Informática y Continuidad del Negocio
- Proyectos y servicios Tercerizados

- Otros Proyectos y adquisiciones
- Plan de Capacitación del Personal de TI
- Cronograma de Actividades
- Presupuesto de TI

El Plan Anual debe ser aprobado formalmente por el Consejo de Administración.

4.2.5. La Inversión en Tecnología de Información

Este es uno de los aspectos más importantes dentro de la gestión de riesgos tecnológicos, ya que las inversiones en TI por lo general, dependiendo de su alcance y ámbito, pueden ser muy costosas y una mala decisión puede representar en grandes pérdidas para la organización desde el punto de vista del negocio y la pérdida de oportunidad asociada, aunque económicamente no lo sea.

Sí, existen organizaciones que realizan inversiones en tecnología pero que muchas veces en la práctica sucede que: no era el hardware adecuado, el software no se adapta a las regulaciones vigentes, las comunicaciones sufren interrupciones inesperadas, etc.

Dentro de las COAC's las inversiones en Tecnología nacen, dependiendo del tipo de adquisición y su monto, como un proyecto formulado por el área de TI, que luego es revisado por el Comité de Informática, que a su vez lo presenta a consideración de la Gerencia General, quien luego de evaluar su factibilidad lo aprueba o lo rechaza. Dependiendo del monto y magnitud del proyecto, es el Consejo de Administración es quien da la última palabra respecto a la ejecución del proyecto en consideración.

Las áreas de TI de las COAC's para las inversiones en tecnología deben tomar en consideración que antes de adquirir el hardware, se debe analizar en forma muy detallada el software que va a correr

dentro de dichos equipos. Es un grave error adquirir primero el hardware y luego el software.

Para el proceso de adquisiciones, el área de TI debe considerar lo siguiente:

- Obtener por lo menos tres cotizaciones de diferentes proveedores.
- Disponer de suficientes proveedores en el mercado.
- En caso de que sólo exista un proveedor en el mercado, verificar que disponga de personal técnico certificado y que se disponga de un proveedor alterno para contingencias.
- En caso de que se entreguen anticipos, solicitar una Póliza de Buen Uso de Anticipo cuya fecha vencimiento sea mayor en por lo menos 60 días respecto a la fecha esperada de entrega.
- Disponer de personal técnico capacitado en el hardware o software que busca adquirirse.
- Solicitar referencias de otros clientes en donde ya estén utilizando el producto ofertado, preferiblemente en empresas del sector financiero.

El Presupuesto de TI debe ser aprobado formalmente por el Consejo de Administración dentro del presupuesto anual de la Entidad.

4.2.6. Gestión del Capital Humano de TI

Este es un aspecto muy importante que debe ser tomado en cuenta por el Jefe del área de TI, debido a que el éxito dentro de la planificación de dicha área recae sobre las personas que la integran. Es por ello, que se debe realizar una completa gestión del recurso humano del área de TI en base a diversos criterios profesionales y de acuerdo a una cultura organizacional que debe establecerse dentro de la Entidad para todos

quienes la integran. A continuación se establecen ciertas recomendaciones prácticas:

1. La Entidad debe formular en forma expresa su misión, visión, valores y un código de ética que debe ser conocido y practicado por todos quienes la componen.
2. El área de TI debe en base a su código de ética general, formular su propio código de ética enfocado de manera más detallada y específica a ciertos principios de confidencialidad, responsabilidad, disponibilidad, trabajo bajo presión y sumisión al control y evaluación continua.
3. Se deben realizar planes de capacitación para la actualización de los conocimientos y destrezas técnicas de los miembros del área de TI.
4. Se deben formalizar en forma muy detallada y específica las responsabilidades, funciones y tareas de cada miembro del área de TI.
5. Se deben realizar evaluaciones de desempeño periódicas del personal del Departamento de Sistemas.

Cabe destacar que debido a la alta presión a la que es sometido el personal del área de TI pudieran existir diversas alteraciones en su conducta y desempeño; por ello, es recomendable que periódicamente se realicen charlas motivacionales, se otorguen bonos por buen desempeño y logro de objetivos e incluso, que se realicen reuniones de trabajo en donde la Alta Dirección reconozca y encomie los logros y desempeño del personal de TI.

4.3. La Seguridad de la Información y la Alta Disponibilidad

4.3.1. La Información como activo del negocio

De acuerdo a la ISO 17799, la información es un activo, que tal como otros importantes activos del negocio, tiene valor para una empresa y consecuentemente requiere ser protegida adecuadamente.

La información dentro de la organización puede estar en diferentes medios: impresa o escrita, medios magnéticos, vídeos y grabaciones, verbal, etc. Por tanto, cuando se habla de que se debe proteger la información, abarca todos los medios sobre los cuales existe información importante para la organización. Las Instituciones Financieras deben preservar sus registros históricos por lo menos seis años de acuerdo a lo establecido por la Superintendencia de Bancos en su Catálogo de Resoluciones, *Libro I.- Normas Generales Para La Aplicación De La Ley General De Instituciones Del Sistema Financiero.- Titulo XII.- De La Información Y Publicidad.- Capitulo II.- Normas Para La Conservación De Los Archivos En Sistemas De Microfilmación, Magneto - Ópticos U Ópticos.- Sección I.- De Los Procedimientos Generales.*

Es por ello, que la Alta Gerencia debe establecer una serie de políticas, procesos y procedimientos que garanticen un adecuado uso y protección de la información. Se debe definir a un ***Propietario de la Información*** que sea el responsable de establecer las acciones necesarias para cumplir con dichas políticas. Adicionalmente, será quien clasifique y determine su acceso a la información de acuerdo a su importancia y criticidad para la organización.

Esto quiere decir que el Propietario de la Información buscará que la información sea confidencial, íntegra y disponible dentro de la organización. Para ello, deberá procurar que exista dentro de la organización una fuerte cultura enfocada a dicho objetivo que involucre a todos quienes forman parte de la Entidad. Además deberá contar con herramientas tecnológicas suficientes para lograr que la información sea accedida solo a personal autorizado, que la información sea confiable e íntegra desde su ingreso hasta su procesamiento y almacenamiento y que esté disponible cuando se la necesite.

4.3.2. La Política de Seguridad

La Alta Gerencia deberá formular una política clara de seguridad de la información que refleje su compromiso y apoyo hacia una gestión de TI sustentable, segura y disponible. Dicha política debe ser difundida a todos los miembros de la organización y deberá ser el pilar fundamental sobre el que se basen todas las demás políticas y procedimientos de seguridad de la información.

La Política de Seguridad, entre otras cosas, debe contener lo siguiente:

- Una declaración expresa sobre la importancia de la seguridad de la información para la organización y un compromiso de todos sus miembros a cumplirla (en especial de la Alta Gerencia).
- Objetivos y alcance de la Política de Seguridad.
- Responsables de la gestión de la seguridad de la información.
- Lineamientos generales de seguridad de la información adoptados por la organización.

El Código de Ética de la Entidad debe considerar la importancia y el compromiso del empleado hacia la seguridad de la información.

4.3.3. Organización de la Seguridad

Es necesario que las COAC's prioricen dentro de la gestión de riesgos tecnológicos, definir responsables de cada uno de los recursos tecnológicos, de la información y de los procesos críticos sobre los que se basa la operatividad del negocio.

Esto quiere decir, que se debe determinar quiénes serán los responsables del control de los activos, de la asignación de los roles y perfiles, de la confidencialidad de la información, de la definición y control de los procesos y operaciones, de la seguridad de las redes y comunicaciones, etc.

Para ello, es necesario que se armen equipos de trabajo relacionados con cada una de las áreas objeto del análisis para definir el personal adecuado para cada una de esas funciones de responsables de la seguridad. En muchos casos, será necesaria la asesoría de empresas externas, de instituciones amigas, de las asociaciones a las cuales pertenezca la Entidad, de los auditores externos e incluso de los organismos de control.

Dentro de esta organización de la seguridad, es necesaria la definición de un Oficial o Administrador de la Seguridad quien es el responsable de que se implementen y se cumplan las políticas y controles de seguridad de la tecnología de información. Dicho rol en muchas COAC's recae sobre el Jefe de Riesgos, aunque sería más conveniente que sea ejercido por una persona distinta quien se enfoque solamente a realizar dicho trabajo.

4.3.4. Clasificación y Control de los Activos

Este es otro de los aspectos muy importantes que deben ser considerados dentro de la gestión de riesgos de TI, debido a que se deben evaluar los mecanismos o controles necesarios para proteger en general los activos de la Entidad y en forma específica los recursos de TI. Al hablar de recursos de TI, no solo abarca el hardware y software sino también la información almacenada en medios físicos y electrónicos.

Es necesario que el área de TI mantenga inventarios de hardware actualizados y controlados que permitan conocer los activos disponibles, sus características técnicas, la fecha de adquisición, vigencia de la garantía del fabricante, ubicación, el usuario asignado a dicho activo, registro de los mantenimientos realizados, etc.

En el caso de la información, ésta debe ser clasificada de acuerdo a su grado de confidencialidad y acceso, el medio en el que se encuentra

almacenado, el propietario de los datos, personas que tienen derecho a su acceso, los medios de respaldo existentes, entre otras cosas.

Una clasificación de la información generalmente aceptada en Entidades Financieras y organizaciones en general, es la siguiente:

- **Público o de Acceso Irrestricto:** Es información disponible para los clientes, socios y público en general. Ejemplo: Balances, Estados de resultados, Transparencia de la información.

- **Privada o de Uso restringido:** Es información que es de uso interno del personal de la organización con accesos formalmente definidos y autorizados. Ejemplo: Diarios contables, información de crédito, transacciones y operaciones diarias.

- **Confidencial o de Alta Privacidad:** El acceso es muy limitado a cierto personal autorizado bajo estrictas normas de control de acceso. Ejemplo: Planes estratégicos y de negocios, nuevos productos y servicios futuros, sigilo bancario, sueldos, etc.

Para cada categoría y sus distintos niveles, se debe establecer los riesgos a los cuales está expuesta la información, su probabilidad de ocurrencia y los controles preventivos y correctivos necesarios para salvaguardarla.

Una vez que la información ha sido clasificada y evaluada desde el punto de vista del riesgo a las cuales pudiera estar expuesta, cuantificado las pérdidas e impacto asociado que pudiera resultar ante un acceso no autorizado o ante una catástrofe y definido los responsables o dueños de los datos; se deberá diseñar una matriz de roles y perfiles asociado a cada categoría y tipo de datos, de tal manera, que se defina quién tiene acceso a cada parte de la información de la Entidad, en forma detallada y específica,

incluyéndose adicionalmente el nivel de acceso otorgado: Ingreso, Consulta, Edición y Eliminación.

Bajo dicha estructura de clasificación de la información deberá basarse todos los futuros desarrollos de aplicaciones de la Entidad. El Jefe de Riesgo, El Jefe de Operaciones y el Auditor Informático tienen un rol muy importante dentro de esta etapa de administración de la información. Sobre ellos también recae la responsabilidad de realizar campañas de capacitación sobre dicha clasificación a los Usuarios de la información.

4.3.5. Aspectos humanos de la Seguridad

La administración de los aspectos humanos de seguridad es muy importante dentro del contexto global de gestión de riesgos, ya que son las personas quienes pondrán en práctica las políticas y normas de seguridad y de igual manera, serán las que podrían incumplirlas. Es por ello, que es necesario disponer de un adecuado proceso de selección, incorporación, capacitación, evaluación y egreso del personal, que permita una correcta administración del capital humano, sobre todo cuando se trata del personal del área de tecnología.

Las COAC's deberán establecer formalmente el perfil de cada puesto de trabajo en cada una de las áreas desde las áreas operativas hasta las ejecutivas, para ello, los dueños de los datos y el Jefe de Seguridad deberán trabajar con el área de Recursos Humanos para definir el nivel académico, experiencia, personalidad, y otros aspectos que deberán cumplir los aspirantes a los diferentes puestos del negocio.

Una práctica sana al momento de incorporar a un nuevo miembro de la organización, es proporcionarle las políticas de seguridad de la información y el Código de Ética interno con el objetivo de que desde el inicio de sus funciones, dicho miembro conozca las políticas internas, la cultura organizacional y las responsabilidades que debe

asumir. Debe formalizarse un Acta de Confidencialidad de la Información y otra de Conocimiento de las Políticas Internas, firmado por el nuevo empleado, que garantice que el funcionario conoce y se compromete a cumplir dichas políticas internas.

Por otro lado, es importante que se planifique tomando en consideración las necesidades y objetivos de la organización, los cursos y seminarios de capacitación para el personal del área de TI.

De igual forma, es necesario que se realicen evaluaciones periódicas al personal del área de TI, en donde se tome en cuenta desempeño profesional, cumplimiento, responsabilidad, puntualidad, organización, respeto a la jerarquía, calidad del trabajo entregado, proactividad, autoeducación personal, entre otras cosas.

Es importante que se recalque constantemente al personal de TI que las aplicaciones y bases de datos son de propiedad exclusiva de la Entidad y que por ningún motivo puede ser prestado, compartido o comercializado a terceras personas. Para ello, las Actas de Confidencialidad deben ser muy claras y detalladas al respecto. Dicha confidencialidad debe perdurar inclusive luego de haber salido de la Entidad.

En la práctica, si una persona es separada de la Entidad o renuncia por su propia iniciativa, dicha persona no puede extraer ningún tipo de información escrita o electrónica de la organización, a pesar que haya sido creada o diseñada por aquella persona. ***La información es un Activo de la Entidad,*** por tanto, dicho funcionario no tiene derecho alguno para que se apropie de ella.

Otro aspecto importante que se debe tomar en cuenta es cómo reaccionará la Entidad frente a incidentes de seguridad de la información cometidas por errores, irresponsabilidad o de forma intencional por parte de los trabajadores. Es por ello, que la Alta

Gerencia debe establecer una adecuada política disciplinaria para los miembros de la Entidad, que advierta y sancione los distintos tipos de violaciones a la seguridad y así mismo, las sanciones vayan de acuerdo a la gravedad de la falta cometida.

4.3.6. Seguridad Física y Ambiental

Es importante que dentro de la Entidad se defina para cada área un nivel de restricción en el acceso, de tal manera, que se protejan las áreas críticas contra el acceso no autorizado. En este sentido, se podría clasificar las áreas como públicas, bajo autorización y restringidas. Por ejemplo en el caso de COAC, las áreas *públicas* serían las de atención al público para transacciones por ventanillas, créditos y servicio al cliente; las áreas de *bajo autorización,* serían las oficinas administrativas de ejecutivos de nivel medio y alto, y las de staff; mientas que en el caso de las áreas *restringidas*, serían las áreas de bóvedas, sistemas, tesorería, contabilidad, entre otras.

En el caso de las áreas con acceso bajo autorización, es recomendable disponer de controles mínimos de entrada como lectores de tarjeta y cerraduras de seguridad media. Por otro lado, en el caso de las áreas de acceso restringido, se pueden implementar lectores biométricos, puertas blindadas y cámaras de seguridad.

Al respecto, es muy importante, la implementación de sistemas de seguridad electrónica que podría ser monitoreado por una empresa externa de seguridad armada y física, o en el mejor de los casos a través de una consola de seguridad centralizado que disponga de software de administración remota de los dispositivos de seguridad electrónica y acceso a las cámaras de seguridad.

En áreas como el centro de cómputo, es recomendable que se instalen dispositivos como sensores de humo, medidores de la temperatura y humedad, sensores de movimiento y hasta cámaras de seguridad. Hay

que recordar que en el caso de las COAC's y la mayoría de las organizaciones, el centro de cómputo es el Core del negocio y como tal, debe disponer de toda una serie de dispositivos y controles que garanticen su seguridad.

Respecto al control de temperatura, existen acondicionadores de aire de precisión, que solamente necesitan mantenimiento cada 6 u 8 años, cuya capacidad de trabajo es 7x24x365 y son capaces de mantener la humedad en condiciones adecuadas para los equipos de computación del centro de cómputo.

4.3.7. Control de Accesos Lógicos

El control de acceso lógico es muy importante a nivel de toda la organización, tanto como lo es el control de acceso físico a las áreas críticas de la Entidad. Por ello, el Comité de Informática deberá establecer adecuadas políticas de control interno para garantizar un adecuado acceso a los recursos del negocio.

El manejo adecuado de los perfiles de usuario para el acceso a la información y que fue analizado anteriormente, es una de las tareas más importantes dentro del control de acceso, ya que ese es el punto de partida para lo que serán los roles y permisos que se generen en delante de las aplicaciones y entorno de red de la Entidad. Es por ello, que se deben establecer procedimientos formales para la creación de los Usuarios dentro las aplicaciones y demás recursos tecnológicos. Cuando se desea contratar a una persona dentro de una Entidad Financiera, luego de pasar la fase de selección y entrenamiento, se la debe concientizar y responsabilizar por las atribuciones en el acceso a la información que tendrá en adelante.

Dentro de las COAC's el Jefe de Riesgos cumple una función muy importante dentro del proceso de creación de Usuarios, ya que por lo general hace sus veces de Oficial de Seguridad y como tal, es quien administra los accesos, los perfiles y, las altas y bajas dentro de las

aplicaciones. Para el efecto, toda alta o baja de usuarios debe ser adecuadamente documentada y registrada por el rol de Oficial de Seguridad y auditada por el Auditor de Sistemas. Los dueños de los datos a su vez, deberán monitorear y supervisar que la información es accesada en forma correcta y segura.

Por otro lado, el Jefe de Riesgos procurará anualmente que todos los Usuarios firmen un Acta de Responsabilidad y Privacidad en el Uso de sus Cuentas de Usuario, en donde se establezcan las políticas y lineamientos en el uso de contraseñas y sobre medidas preventivas para evitar perder la contraseña o sea accedida por terceros a través de ingeniería social.

Respecto al manejo de las Cuentas de Usuario y de las contraseñas se recomienda lo siguiente:

- Las Cuentas de Usuario deben ser asignadas a un solo Usuario.
- Cada Usuario debe estar asociado a un solo perfil. Los perfiles a su vez deben estar compuestas por roles. Se deberá procurar que exista una adecuada segregación de funciones en la asignación de roles y perfiles a los Usuarios.
- Durante el inicio de sesión el usuario y la contraseña deben viajar encriptados a través de la red de datos.
- La longitud de las contraseñas debe ser de por lo menos seis caracteres y a su vez debe estar compuesta por letras, números y símbolos especiales.
- Las contraseñas deben ser ocultadas al Usuario mientras son escritas.
- En el primer inicio de sesión debe ser cambiada la contraseña por el Usuario.
- Las contraseñas deben ser cambiadas periódicamente, cada 30 o 60 días o cuando el Usuario lo requiera hacer sin límites

de veces. Una vez definida la política para la expiración de contraseñas, el recordatorio de cambio de contraseña debe ser automático para el Usuario.

- El acceso a los recursos tecnológicos debe estar restringidos a horarios y días específicos para cada perfil de Usuario.
- En los sistemas de información a más del Usuario y la Contraseña, podría validarse la dirección IP o el MAC Address de la estación de trabajo.
- Dentro de las políticas de red debería establecerse que cada cierto tiempo de inactividad el equipo se bloquee a través del protector de pantalla el cual deberá estar protegido por la contraseña de inicio de sesión.

4.3.8. Plan de Continuidad del Negocio

En forma tradicional las áreas de TI han diseñado un plan de contingencias contra incidentes que les permita definir una serie de acciones tanto preventivas como correctivas frente a diferentes eventos como incendios, inundaciones, fallas eléctricas, entre otras, con el objetivo de garantizar la continuidad de los servicios de TI, lo que en la práctica ha dado buenos resultados a las Entidades para afrontar las diferentes contingencias a las que pudieran estar expuestas.

Sin embargo, al hablar de una adecuada e integral administración del riesgo, es necesario que la Entidad diseñe un Plan de Continuidad del Negocio que reúna en forma cabal los diferentes planes de contingencia de todas las áreas que la integran, de tal manera que se garantice la continuidad de las operaciones a pesar de una contingencia grave. Esto quiere decir, que se disponga de un plan unificado que indique las acciones que debe seguir cada departamento, sucursal, agencia y unidad de apoyo frente a un evento de riesgo que pudiera afectar a la Entidad de forma grave. La intención de esto, es

que no se interrumpa las operaciones de la Entidad Financiera y poder cumplir con sus clientes frente a cualquier tipo de escenario adverso.

Para la elaboración del Plan de Continuidad del Negocio, es necesaria la participación de la Alta Dirección, los Jefes Departamentales, el Jefe de Riesgos, el Jefe de Seguridad Informática, el Auditor Interno, el Auditor de Sistemas, el Jefe de Operaciones y demás personal de apoyo que tenga relación con la seguridad física, logística, mantenimiento y aprovisionamiento.

El diseño de las acciones preventivas y correctivas frente a los diversos escenarios de desastre o evento contingente debe ser realizarse en base a cada línea de negocio y no en forma departamental; esto quiere decir que el Plan de Continuidad del Negocio no consiste en unir en un solo documento el plan de contingencias de cada departamento; sino en definir las acciones necesarias para garantizar las operaciones de ventanillas, servicio al cliente, crédito y cartera, manejo de inversiones, banca electrónica, entre otros.

El Plan de Continuidad del Negocio deberá estar basado en los análisis de riesgos previamente realizados durante el proceso de planificación de la gestión de riesgos y estar formalmente documentada y aprobada por el Consejo de Administración. En forma periódica se realizaran pruebas de validación de la efectividad del plan y se realizarán las actualizaciones necesarias para garantizar su idoneidad.

Para disponer de un Plan de Continuidad del Negocio altamente efectivo debe considerarse lo siguiente:

- Debe ser diseñado por personal jerárquico clave interdisciplinario e interdepartamental que conozca cada proceso de la Entidad.

- Definir el Objetivo de Punto de Recuperación y el Objetivo de Tiempo de Recuperación.
- El Plan debe determinar en forma específica las acciones que deben tomarse en forma preventiva y correctiva y quién deberá ejecutarlas, cómo y cuándo.
- TODO el personal debe conocer el Plan de Continuidad del Negocio y dominar las responsabilidades asignadas. Esto incluye a los proveedores de servicios tercerizados.
- El Plan de Continuidad del Negocio debe ser probado por lo menos una vez al año, sino su probabilidad de efectividad se reduce enormemente.
- El Plan debe especificar como mínimo: una aseguradora para todos los activos de la Entidad, un lugar donde funcionar en caso de que la Oficina Matriz haya sido destruida, un Centro de Procesamiento Electrónico de Datos alterno y los procesos críticos de negocio mínimos que deberán ser "levantados" en forma prioritaria.

El Plan de Continuidad del negocio deberá ser aprobado formalmente por el Consejo de Administración de la Entidad.

4.4. La Entrega de Servicios y la Calidad de los Procesos de Tecnología

4.4.1. El Manual de Políticas y Procedimientos Informáticos

Es verdad que muchas organizaciones funcionan bien y generan ganancias a nivel tecnológico y operativo de manera informal sin disponer de manuales, políticas ni procedimientos. Sin embargo, en el caso de las Entidades Financieras, es necesario de que todas sus políticas y procedimientos estén debidamente formalizados por escrito y aprobados por la Alta Dirección; en el caso de las COAC's por el Consejo de Administración.

Dicho manual de políticas y procedimientos informáticos deberá ser elaborado por el Jefe de Sistemas considerando las diferentes áreas de

acción de las cuales es responsable el Departamento o Unidad de Sistemas. El Comité de Informática revisará y recomendará las modificaciones necesarias al manual de políticas y procedimientos en base a la diversidad de criterios profesionales de cada uno de sus miembros. Por ejemplo, el representante de los usuarios hará recomendaciones sobre la calidad del servicio y control de requerimientos, mientras el Auditor de Sistemas se enfocará hacia una adecuada segregación de funciones, el control en el ciclo de vida de los sistemas, la seguridad, entre otros aspectos.

Una vez revisado y aprobado por el Comité de Informática deberá pasar a consideración del Consejo de Administración para una revisión final y para su posterior aprobación y puesta en vigencia. Dicho manual una vez puesto en vigencia deberá ser difundido a todos los miembros del Departamento de Sistemas y deberán firmar un acta de compromiso y responsabilidad en donde afirmen haber conocido, leído y comprendido el manual de políticas y procedimientos informáticos y que por otro lado, se comprometen a cumplirlo cabalmente, aceptando cualquier tipo de sanción o multa por su incumplimiento.

Respecto al contenido del manual de políticas y procedimientos informáticos, dependerá de cada Entidad y estará diseñado de acuerdo a su tamaño y servicios. Sin embargo, en forma general, un manual de políticas y procedimientos informáticos recomendamos disponga de lo siguiente:

1. Objetivos del manual
2. Alcance
3. Términos generales
4. Planificación de Tecnología de Información
5. Adquisición y Administración de recursos tecnológicos
6. Desarrollo y Mantenimiento de Sistemas de Información
7. Contratos y Servicios provistos por Terceros

8. Alta disponibilidad y Continuidad del negocio
9. Servicios y soporte a Usuarios
10. Calidad y Mejora Continua
11. Políticas y Procedimientos para Usuarios

Con el objetivo de lograr un manejo óptimo del manual de políticas y procedimientos informáticos, éste podrá dividirse por secciones para que sea más manejable y fácil de usar. Nótese que se recomienda una sección de políticas y procedimientos para los Usuarios. Esto se debe a que se deben establecer y difundir a todos los Usuarios de los recursos tecnológicos de la Entidad sobre sus responsabilidades, obligaciones y procedimientos a seguir.

4.4.2. El Manual Orgánico Funcional

El Comité de Informática tiene la responsabilidad de definir, recomendar y mejorar continuamente el Manual Orgánico Funcional del área de TI; el cual, delinea en forma específica y detallada las funciones, responsabilidades y tareas del personal de tecnología. Dicho manual incluye también el Organigrama del área de TI.

Se deberá procurar que todo el personal de TI conozca sus funciones y responsabilidades, las mismas que deberán ser adecuadamente delimitadas por el Comité de Informática, de tal manera que se evite la duplicación de funciones y que exista la segregación de funciones incompatibles que garantice que en los diversos procesos de TI sean realizadas bajo estrictos controles de seguridad. Por ejemplo, debe evitarse que un mismo funcionario sea quien desarrolle, haga las pruebas y ponga en producción las aplicaciones.

Las funciones asignadas a cada funcionario de TI deben ser realizadas bajo un enfoque de servicio y resolución de conflictos que garantice que el personal de TI tenga entre sus funciones la resolución de problemas, la ética, una orientación hacia la calidad y atención al Usuario.

Adicionalmente, se debe dejar claro la posición jerárquica de cada miembro del área de TI sepa a quien debe obedecer y rendir cuentas y así mismo a quien debe dirigir y controlar. El Organigrama Funcional y jerárquico debe formar parte del Manual de Funciones de TI. Si se desea ir más allá, es recomendable que incluso se realice un análisis de la relación funcional con otros departamentos, identificando con qué Departamentos y cargo el área de TI debe interactuar para brindar soporte y atender nuevos requerimientos de hardware y software.

4.4.3. Desarrollo y Mantenimiento de los Sistemas de Información

Dentro de la administración del riesgo relacionado al desarrollo y mantenimiento de sistemas de información se debe destacar la necesidad de formalizar las políticas, procedimientos y estándares de dichos procesos con la finalidad de garantizar la uniformidad en el desarrollo de las aplicaciones informáticas, mejorar la eficiencia y permitir su control posterior.

Es particularmente conocido que estadísticamente muy pocos proyectos de desarrollo de software tienen 100% de éxito y cumplen con las expectativas propuestas; es por ello, que dentro de las COAC's sin importar el tamaño del área de desarrollo de aplicaciones, la planificación es un factor de éxito muy importante que hay que tener en cuenta para una adecuada administración del desarrollo de aplicaciones.

Dicha planificación debe considerar los recursos necesarios, una correcta asignación de tareas y una adecuada comunicación con los Usuarios que hicieron los requerimientos de desarrollo. Esto es particularmente importante para evitar conflictos entre los jefes departamentales y el Jefe de Sistemas quien debe dar respuesta a los reclamos de los Usuarios frente a los atrasos en el cumplimiento de los requerimientos de software.

Por otro lado, debe definirse formalmente las políticas de seguridad dentro del desarrollo de las aplicaciones; lo cual incluye controles de validación, técnicas de software seguro, prohibición de código muerto o inactivo, prevención de entradas de datos inseguros y demás formas de prevención y garantía de la calidad y seguridad del código fuente.

Respecto a los cambios en las aplicaciones, debe procurarse que se lleve a cabo un adecuado control de los cambios realizados a las aplicaciones y que exista una debida segregación de los ambientes de desarrollo, pruebas, preproducción y producción. Una misma persona no puede ser responsable de todo el proceso de cambio a las aplicaciones porque eso conlleva un riesgo de seguridad en las aplicaciones. En el caso de las cooperativas pequeñas, donde solamente exista una persona para el área de TI, es recomendable que el Jefe de Riesgos realice las funciones de control y supervisión de los cambios a las aplicaciones.

Si el desarrollo o mantenimiento de la aplicación está a cargo de terceros, se debe procurar que existan contratos claros y bien definidos sobre las responsabilidades del proveedor, tiempos de entrega, calidad de software, actualizaciones, multas por retrasos, propiedad intelectual y custodia del código fuente, acuerdos de confidencialidad, personal a cargo del proyecto, multas por incumplimiento, entre otras cosas. El área legal y de auditoría juegan un papel muy importante durante todo el proyecto para su cumplimiento.

4.4.4. Servicios brindados por Terceros

En ocasiones, es conveniente que una empresa externa realice algunos de los servicios de tecnología de la Entidad, sobre todo cuando no se dispone de suficiente personal técnico. Sin embargo, hay que cuidar mucho del grado de apertura que se le va a dar a dichas empresas tercerizadoras, especialmente en lo referente a información considerada confidencial por la Entidad.

Para ello, se debe partir de una evaluación de la información que podría estar expuesta hacia la empresa tercerizadora como parte de sus funciones dentro del servicio que va a brindar. Dicha información debe ser catalogada como confidencial, privada o pública (dependerá de cada Entidad) y de acuerdo a dicho análisis, determinar los controles para garantizar la restricción o acceso a la información por parte de terceros.

Es importante que como parte del contrato entre las partes, se formalice un ***Convenio de Confidencialidad de la Información,*** que obligue a la empresa tercerizadora a no difundir la información a la que tiene acceso y de implementar los controles necesarios para que de igual forma, sus empleados no divulguen dicha información, bajo parámetros de responsabilidad civil y penal.

Adicionalmente, es recomendable que se permita el acceso a las instalaciones de la empresa tercerizadora, de los auditores internos y externos de la Entidad con el objetivo de constatar que dicha empresa cumple con los requerimientos mínimos de seguridad y con la infraestructura necesaria para garantizar un adecuado servicio y soporte.

En este sentido, la Entidad debe diseñar un manual general de políticas y procedimientos para contratación de productos y servicios de terceros, que gobierne todos los diferentes tipos de adquisiciones que se realicen en los diferentes departamentos o áreas de la organización. En particular, habrá dentro de dicho manual un capítulo, sección o submanual de adquisiciones de tecnología de información en el que se establecerán políticas y procedimientos detallados y específicos sobre las adquisiciones de hardware, software, redes y demás servicios relacionados.

4.4.5. Las Redes y Comunicaciones

La gestión de riesgos en lo relacionado con redes y comunicaciones es una de las tareas más complejas y de mayor profundidad dentro de las COAC's debido a las diferentes amenazas a las que están expuestas en la actualidad las tecnologías de redes y comunicaciones y por otro lado, a lo atractivo que es para muchas personas poder vulnerar las seguridades de la red de las Entidades Financieras.

Una vez identificadas las amenazas a las cuales están expuestos los procesos y recursos de TI relacionados con las redes y comunicaciones, es necesario realizar una planificación para implementar las medidas preventivas y correctivas que permitan afrontar dichas amenazas y que garanticen la operatividad y continuidad de los procesos de redes y comunicaciones de manera segura, eficiente y confiable.

En este sentido, es necesaria la participación multidisciplinaria del Jefe de Sistemas, el Jefe de Riesgos y el Auditor de Sistemas para determinar los lineamientos, políticas y procedimientos de administración y sobre todo respecto al control y seguridad de los recursos de redes y comunicaciones; participar en su implementación y monitorear su cumplimiento y mejora continua.

Al momento de realizar la planificación de la administración del riesgo en las redes y comunicaciones de la Entidad se deben considerar los elementos que permitan una adecuada gestión de la red, disponer un adecuado inventario de los recursos de red disponibles y la arquitectura de información de la Entidad. Así mismo, se deberá definir una estrategia para la prevención y resolución de problemas y una política de alta disponibilidad para garantizar la continuidad de los recursos de red y comunicaciones.

Por otro lado, se deberá definir los proveedores principales y secundarios de los servicios tercerizados y de soporte técnico que permitan obtener una respuesta rápida ante posibles contingencias. La definición de estándares de comunicación, de equipos activos y pasivos, de software de administración y monitoreo de red, de protocolos y de ejecución de operaciones, es otro de los aspectos importantes de considerar dentro de la planificación para la administración del riesgo de redes y comunicaciones.

La administración de riesgos de redes y comunicaciones podría enfocarse en las siguientes áreas o aspectos de control:

- Gestión de Riesgo de la Planificación y Organización.
- Gestión de Riesgo de la Red Física
- Gestión de Riesgo de la Red Lógica

En cuanto a la Gestión de Riesgo de la Planificación y Organización se recomienda lo siguiente:

- La existencia de un cargo de Administración de Redes y Comunicaciones cuyas funciones estén claramente segregadas y diferenciadas a las del Administrador de Sistemas, Operaciones, Bases de Datos u otro cargo dentro del área de TI, de tal manera que se evite la incompatibilidad de funciones.
- Políticas y procedimientos claramente definidos respecto a la administración, operación, monitoreo, calidad, seguridad y de recuperación frente a desastres, para cada uno de los servicios de redes y comunicaciones. Esto incluye la formalización de una arquitectura de redes y comunicaciones y el diseño de los diagramas de las redes LAN y WAN.
- Políticas y procedimientos formalmente definidos para el registro, seguimiento y corrección de incidentes para garantizar que se tomen medidas de acción preventivas para

disminuir su probabilidad de ocurrencia y mitigar su impacto en el futuro.

- Una política de seguridad y alta disponibilidad para garantizar que la Entidad asuma la responsabilidad de asegurar la inversión en nuevas tecnologías de hardware y software que le permitan disminuir el riesgo de ataques externos e internos contra la seguridad de sus aplicaciones, servidores y demás recursos conectados a la red de datos.
- Una participación proactiva del Administrador de Redes y Comunicaciones dentro del diseño y mantenimiento de las aplicaciones de software mediante la recomendación de controles y medidas de seguridad para garantizar la eficiencia, calidad e integridad de la información mientras es transmitida a través de la red de datos.
- De existir varias personas dentro de la función de redes y comunicaciones, deberá establecerse las funciones, responsabilidades y procesos de cada cargo y definir un orden jerárquico funcional.
- Formalizar los procesos, actividades y tareas del área o función de redes y comunicaciones; así como los estándares de cableado estructurado, hardware (equipos activos) y software a seguirse; y, los niveles de autorización y acceso a la red de datos.
- Contratos debidamente firmados entre la Entidad y sus diversos proveedores de servicios de redes y comunicaciones tercerizados, que incluyan acuerdos de confidencialidad, niveles de calidad servicio (up-time) y penalizaciones por incumplimiento.

Respecto a la Gestión de Riesgo de la Red Física es importante mencionar:

- Deben existir controles adecuados para garantizar la seguridad de los equipos principales de redes y comunicaciones ubicados en el Centro de Cómputo contra accesos no autorizados.
- El cableado estructurado deberá estar protegido por canaletas (dentro de la Oficina) y por tubería EMT (fuera de la Oficina) para garantizar que no sean manipulados, dañados o "pinchados".
- Realizar pruebas periódicas al cableado de datos mediante dispositivos de control y monitoreo para garantizar su correcto funcionamiento y calidad de transmisión.
- Disponer de acometidas de cableado estructurado de backup para ser utilizados en caso de contingencias.
- Los equipos de comunicaciones deben ser ubicados en racks cerrados con llave en ambientes seguros con condiciones ambientales adecuadas y bajo estándares de instalación, adecuadamente organizados y ubicados.
- Seleccionar en forma minuciosa al personal externo de electricidad, mantenimiento y de telefonía e implementar los controles necesarios de vigilancia y supervisión cuando estos realicen trabajos en el Entidad, tanto dentro como fuera de los horarios de oficina.
- Los Patch Panel de Enlace y especialmente el Patch Panel de Core, Switches y acometidas de cableado estructurado deberán estar etiquetados para identificar cada puerto, dispositivo y cable instalado dentro de la red de datos.
- Se deberá procurar mantener un centro de comunicaciones alterno fuera de la Oficina Matriz para casos graves de desastre, así como enlaces de transmisión de datos y de Internet de backup.

Sobre la Gestión de Riesgo de la Red Lógica se exhorta tomar en cuenta:

- La red de datos debe ser administrada a través de un Sistema operativo de red fiable, seguro y debidamente actualizado en sus versiones y parches de seguridad.
- Deberán definirse políticas de roles, funciones y usuarios para el acceso a la red. Los recursos compartidos deben estar protegidos solo para personal autorizado.
- Disponer de herramientas de software que permitan monitorear alguna actividad sospechosa o inusual en la red o en las computadoras que pertenecen a ella.
- Controles para evitar que existan ataques de "broadcast" en la red que pudieran hacer caer las conexiones.
- Establecer políticas de cambio de contraseñas de los usuarios de la red preferiblemente cada 30 días.
- Los accesos a las redes inalámbricas debe ser realizado validando usuario, contraseña y Mac Address del equipo. Se deberá permitir el acceso solo a los computadores de la Entidad.
- Se debe llevar bitácoras de registro de novedades, incidentes o eventos suscitados en la red de datos o comunicaciones.
- La información a través de las redes LAN y WAN de la Entidad deben viajar encriptados para evitar que puedan ser interceptadas e interpretadas.
- Se deberá disponer de suficientes controles de ancho de banda y calidad de servicio en los enlaces de transmisión de datos para la conexión entre el Servidor de Producción de base de datos y el de Standby ubicado en otra oficina.
- El acceso a internet debe ser administrado a través de un Servidor Proxy con suficientes restricciones para evitar la descarga de música y pornografía y acceso sólo a páginas relacionadas con el giro del negocio de la Entidad.
- Deben existir políticas para evitar la instalación de software ilegal o la inserción de dispositivos USB externos en las terminales de la red.

- Se deben implementar sistemas de control para evitar el SPAM o cualquier otro tipo de amenazas como virus, gusanos y troyanos. Se debe disponer de un Sistema de prevención de Intrusos.
- Los enlaces VPN deben estar controlados y monitoreados para garantizar su uso debido y deben ser habilitados solo cuando sea necesario y bajo la autorización del jefe de Seguridad o Jefe de Riesgos.
- Verificar que no existan puertos vulnerables y abiertos en los diferentes computadores personales, servidores u otros equipos conectados a la red que pudieran ocasionar una falla de seguridad.
- Realizar revisiones de "Ethical hacking" por lo menos una vez al año para verificar que no existan vulnerabilidades de la red a nivel interno y externo.

4.4.6. Servicios de Hosting

En el caso de los servicios de hosting, es necesario que dentro de los contratos firmados entre las partes, se establezcan controles mínimos de seguridad, en cuanto a instalaciones físicas, seguridad en la transmisión de datos, control de acceso a la información, etc., de tal manera que se garantice que la información confidencial de la Entidad estará protegida y restringida contra terceros e incluso para el personal no autorizado dentro de la empresa proveedora. Deberán establecerse minuciosos acuerdos de confidencialidad entre las partes en el que incluso, se proteja la información de la Entidad frente a otros clientes del proveedor.

Una práctica sana podría ser, obviamente previo acuerdo entre las partes, que la Entidad a través de su departamento de auditoría interna, realice por lo menos dos veces al año una visita a las instalaciones del proveedor para constatar las instalaciones, políticas y procedimientos de seguridad que dicha empresa posee. De ser el caso, será necesaria

la asesoría y soporte de un especialista en seguridades de redes y comunicaciones para tales revisiones en las instalaciones del proveedor.

En caso de las Entidades que dependen en gran medida de que sus servicios Web estén disponibles en forma ininterrumpida, es necesario que se dispongan de planes de contingencia actualizados y debidamente formalizados y aprobados, en el que se establezca el proveedor de backup que estará disponible para levantar los servicios Web de la Entidad, para el caso de que el proveedor local tenga una caída de sus servicios debido a contingencias inesperadas o por motivos de mantenimiento. A este respecto, hay que ser enfático en el sentido de que en el contrato de servicio se deben establecer las penalizaciones en caso de caídas del servicio brindado por el proveedor de hosting.

4.4.7. La Mesa de Servicios (Service Desk)

La Mesa de Servicios es un concepto formulado por ITIL para una adecuada gestión de los servicios de TI, en donde se constituye como una interfaz para clientes y usuarios de todos los servicios de TI ofrecidos por la organización, con un enfoque centrado en los procesos del negocio. Brindando entre otras cosas los siguientes servicios:

- Supervisión de los contratos de mantenimiento y niveles de servicio.
- Canalización de las Peticiones de Servicio de los clientes.
- Gestión de las licencias de software.
- Centralización de todos los procesos asociados a la Gestión TI.

La conformación de una Mesa de Servicio requiere de un profundo análisis técnico, logístico y humano para que cumpla en forma efectiva con su propósito de atender en forma eficiente a las

solicitudes de soporte de los usuarios, así como optimizar las operaciones de la organización en base a la solución oportuna de incidentes o eventos técnicos enfocado a sus Usuarios, Clientes y Proveedores de Servicios. Por tal motivo, debe buscarse las siguientes condiciones para el éxito de la Mesa de Servicio:

- Establecer estrictos protocolos de interacción con el cliente.
- Motivar al personal encargado de la relación directa con el cliente.
- Informar a los clientes de los beneficios de este nuevo servicio de atención y soporte.
- Asegurar el compromiso de la dirección con la filosofía del Service Desk.
- Sondear a los clientes para conocer mejor sus expectativas y necesidades.

4.5. El cumplimiento con las regulaciones de los Organismos de Control

El cumplimiento es otro de los aspectos que dentro de la gestión del riesgo operativo debe ser abarcado de forma responsable y minuciosa por las COAC's al igual que el resto de Instituciones Financieras. Esto es particularmente complejo ya que se debe cumplir con diferentes normas, reglamentos y disposiciones emitidas por los Organismos de Control, entre las que se encuentra de forma principal la Superintendencia de Bancos y Seguros.

La Norma principal sobre la cual se basan las operaciones de las COAC's es la Ley General de Instituciones Financieras; la cual, se complementa con las diferentes disposiciones emitidos en forma regular por la Superintendencia de Bancos y Seguros, que de igual manera son de cumplimiento obligatorio. Así mismo, existen disposiciones y reglamentos emitidos por el Banco Central, el Servicio de Rentas Internas y la Unidad de Inteligencia Financiera (antes CONSEP) que deben ser cumplidos por las COAC's.

Por otro lado, existen un considerable número de estructuras de información que deben ser reportadas en forma periódica a los Organismos de Control anteriormente mencionados y cuyo cumplimiento debe ser realizado en plazos previamente establecidos y bajo características técnicas bien definidas por el organismo emisor. Es por ello, que cada Entidad debe establecer políticas y procedimientos formales para vigilar el cumplimiento en el envío de las estructuras ya que su incumplimiento trae consigo multas y sanciones para la Entidad y su representante legal.

El uso de los sistemas de información es esencial para el cumplimiento en el envío de las estructuras de información para su generación, revisión, envío y control. A continuación se presenta un resumen de las estructuras que deben ser reportadas a la Superintendencia de Bancos y Seguros en forma periódica.

Categoría	Estructura	Descripción	Periodicidad
Central de Riesgos	R01	Sujetos de Riesgo	Mensual
Central de Riesgos	R02	Operaciones Concedidas	Mensual
Central de Riesgos	R2A	Reclasificación de cartera	Eventual
Central de Riesgos	R03	Operaciones anteriores	Mensual
Central de Riesgos	R04	Saldos	Mensual
Central de Riesgos	R05	Operaciones canceladas	Mensual
Central de Riesgos	R5A	Operaciones canceladas(semanal)	Semanal
Central de Riesgos	R06	Garantes y Codeudores	Mensual
Central de Riesgos	R07	Garantías	Mensual
Central de Riesgos	R08	Bienes muebles e inmuebles adjudicados	Mensual
Central de Riesgos	R09	Títulos valores adjudicados por pago	Mensual
Central de Riesgos	R13	Otros Riesgos	Mensual
Central de Riesgos	SB231B	Resumen de calificación de otros activos y constitución de provisiones	Trimestral
Riesgos de Mercado y Liquidez	R31	Emisores de Inversiones	Mensual
Riesgos de Mercado y Liquidez	R32	Portafolio de Inversiones	Mensual
Riesgos de Mercado y Liquidez	R33	Saldos de liquidación de inversiones	Mensual
Riesgos de Mercado y Liquidez	R36	Liquidez Estructural	Semanal
Riesgos de Mercado y Liquidez	R38	Detalle de productos	Mensual
Riesgos de Mercado y Liquidez	R41	Brechas de sensibilidad	Mensual
Riesgos de Mercado y Liquidez	R42	Sensibilidad del valor patrimonial y margen	Mensual
Riesgos de Mercado y Liquidez	R45	Brechas de liquidez	Mensual

Riesgos de Mercado y Liquidez	B45	Captaciones por monto Cuenta 21	Mensual
Riesgos de Mercado y Liquidez	B46	Obligaciones financieras Cuenta 26	Mensual
Riesgos de Mercado y Liquidez	B48	Concentración de depósitos de los 100 mayores clientes	Mensual
Detalle de depósitos garantizados	D01	Detalle de depósitos garantizados	Mensual
Catastro Institucional	C11	Nómina de personal	Trimestral
Catastro Institucional	C21	Nómina de ejecutivos, directorios o consejos.	Trimestral
Catastro Institucional	C23	Parientes de Directivos	Trimestral
Catastro Institucional	C41	Auditores Internos	Anual
Catastro Institucional	C01	Nomina de personal actualizado	Eventual
Catastro Institucional	C02	Nomina de ejecutivos, directivos y directorio actual	Eventual
Catastro Institucional	C03	Nomina de parientes directivos directorio actualizado	Eventual
Catastro Institucional	C06	Auditores internos actualizado	Eventual
Transparencia de Información	A01	Tasa de interés pasivas efectivas	Semanal
Transparencia de Información	A05	Cuentas de Ahorro	Semanal
Transparencia de Información	A07	Microempresa - Consumo	Semanal
Estados Financieros	B11	Estados Financieros	Mensual
Estados Financieros	B12	Detalle de Captaciones y Colocaciones	Mensual
Estados Financieros	B13	Balances de Instituciones Financieras	Diario
Estados Financieros	SB203	Estado consolidado anual de cambios en la posición financiera	Mensual
Patrimonio Técnico	B41	Patrimonio técnico requerido y constituido	Mensual
Patrimonio Técnico	B42	Detalle de inversiones en acciones y participaciones	Mensual
Patrimonio Técnico	B43	Anticipo para adquisición de acciones y participaciones de compañías no constituidas	Mensual
Patrimonio Técnico	B44	Detalle de contratos de compra y venta de divisas	Mensual
Patrimonio Técnico	SB229	Relación entre el patrimonio técnico y activos y contingentes ponderados por riesgo	Mensual
Información de la Publicación		Estados financieros e indicadores financieros	Anual
Información de la Publicación		Relación entre el patrimonio técnico y activos y contingentes ponderados por riesgo (publicación)	Anual
Información de la Publicación		Calificación de activos de riesgo (publicación)	Anual
Información de la Publicación		Dictamen de los auditores externos	Anual
Otros Formularios	SB215	Distribución de utilidades	Anual
Otros Formularios	SB250A	Límites de crédito (Art. 72 LGISF)	Mensual
Otros Formularios	SB250B	Límites de crédito (Art. 73 y 74 LGISF)	Mensual
Otros Formularios	SB250C	Límites de crédito (Art. 75 LGISF)	Mensual
Otros Formularios	SB299	Reporte de retención y pago de impuestos	Mensual

Tabla 4.1. Resumen de Estructuras de Información enviadas a la Superintendencia de bancos y Seguros.

4.6. La Administración Integral del Riesgo Tecnológico y su impacto en la cadena de valor del negocio.

A pesar de que la administración del riesgo operativo y tecnológico es una disposición de carácter obligatorio para las entidades financieras en el Ecuador y de forma particular también para las COAC's, su implementación ha significado una excelente oportunidad para dichas entidades de mejorar y formalizar sus procesos; de capacitar y concientizar a su personal; y, de innovar en la seguridad de sus tecnologías de información y comunicaciones.

A través de la aplicación de la Norma 834 emitida por la Superintendencia de bancos y Seguros, las COAC's han comenzado en su mayoría, a definir en forma específica y detallada cada uno sus procesos, los cuales, por mucho tiempo estuvieron informalmente desarrollados, sin conocer el grado de ineficiencia de muchos de ellos o ignorando la exposición al riesgo de muchos procesos mal definidos o estructurados y una falta de medición de los resultados que generaban dichos procesos.

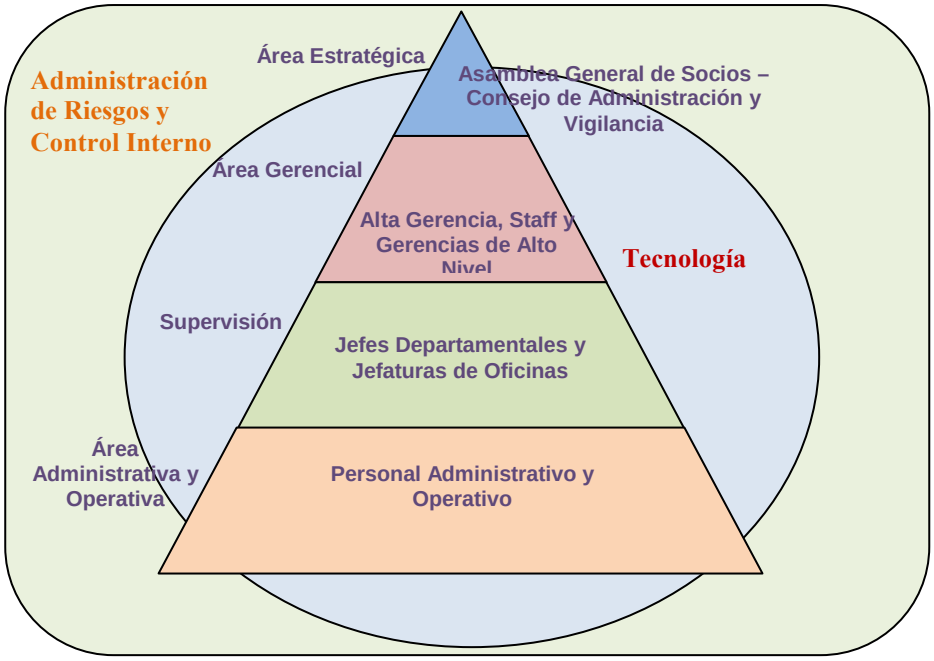


Figura 4.2. Pirámide Organizacional en las COAC's enfocado en la Administración del Riesgo y la Tecnología

Así mismo, en muchas COAC's antes no se tenía una visión clara sobre la importancia de formalizar en forma técnica los diferentes puestos y cargos en dichas entidades, tampoco sobre la importancia de que exista una adecuada segregación de funciones para disminuir el riesgo de fraude o de error, peor aún sobre la necesidad de que exista un entrenamiento continuo para el personal en temas de gestión de riesgos y ética empresarial.

Por otro lado, antes se pensaba que con disponer de un área de tecnología, un sistema transaccional y enlaces de comunicaciones era suficiente para garantizar el correcto funcionamiento y disponibilidad de las operaciones en las COAC's. Sin embargo, ahora existe una conciencia clara y un horizonte por parte de la Alta Dirección sobre su rol preponderante en la gestión de tecnología; sobre la necesidad de invertir y apoyar la seguridad de la información; y, la importancia de disponer de sistemas de hardware, software y comunicaciones redundantes que aseguren la confiabilidad, integridad y disponibilidad de la información, así como la continuidad del negocio.

Figura 4.3. Cadena de Valor en las COAC's

A través de una adecuada gestión del riesgo operativo y tecnológico, las COAC's tienen ante sí una herramienta diferenciadora y estratégica a nivel competitivo, ya que les permite ser más eficientes y productivos al realizar sus operaciones; les da la posibilidad de generar, innovar e implementar

nuevas tecnologías en forma sustentable que les permita ofrecer nuevos productos y servicios bajo niveles óptimos de calidad a sus clientes; así como también, les da la capacidad de garantizar y asegurar a sus clientes que sus recursos e información financiera están bien protegidos.

Los socios y clientes de las COAC's poco a poco van percibiendo los resultados de todo el esfuerzo que realizan sus entidades para cumplir con la administración del riesgo operativo, brindándoles confianza y seguridad de una adecuada administración de sus recursos, permitiendo a las entidades financieras y muy particularmente a las COAC's tener un crecimiento sostenido a nivel financiero y operacional.

Por lo tanto, una adecuada administración del riesgo operativo y tecnológico permite a las COAC's beneficiarse a nivel interno y externo, ya que permite el logro de los objetivos estratégicos, la mejora de los procesos, disminuye la ineficiencia, aumenta la productividad, mejora el control interno, salvaguarda los recursos, garantiza la continuidad del negocio, transmite seguridad y confianza a los clientes y socios, asegura el cumplimiento de las normas y regulaciones de los organismos de Control y permite un crecimiento sostenible en el largo plazo.

Capítulo 5.

Aprovechamiento de los Sistemas de Información en la Administración del Riesgo Operativo Tecnológico de las COAC's

5.1. Tendencias tecnológicas para la administración del Riesgo Operativo Tecnológico

Como hemos visto, los diferentes estándares como COBIT, ITIL e ISO 27001, son una excelente referencia para los directores y Jefes de Sistemas de las Entidades Financieras para la aplicación de políticas y procedimientos adecuados para un gobierno de Tecnología de Información responsable que permita la aplicación de un eficiente control interno de tecnología de información que garantice la seguridad de la información y los recursos tecnológicos.

Para la aplicación de políticas y procedimientos dentro de una adecuada gobernabilidad de TI, es necesaria su formalización a través de su documentación por escrito y la participación del Consejo de Administración para su aprobación y puesta en marcha. Sin embargo, el uso de herramientas informáticas puede ser de gran ayuda para el monitoreo del cumplimiento de dichas políticas.

Tal es así, que existen herramientas de software para la implementación de la normativa COBIT e ITIL, así como para la evaluación de riesgos de tecnología de información y planificación frente a desastres.

5.1.1. COBIT ADVISOR

COBIT Advisor es una herramienta muy útil para el control dentro de la implementación de los objetivos de control de COBIT de especial beneficio para las Entidades Financieras. Entre otras cosas permite:

- Evaluar el proceso de gestión y control de Tecnología de información basado en COBIT.
- Comparar los objetivos de control recomendados por COBIT frente a las políticas y procedimientos de administración de TI de la organización para su alineamiento. Las revisiones se pueden realizar por dominios y objetivos de control. Existen lineamientos de auditoría para guiar el proceso de revisión.
- El control sobre el cumplimiento de los objetivos de control de COBIT se basa en los procesos críticos del negocio, los recursos de TI y los criterios de Información definidos por COBIT.
- Permite hacer un seguimiento mediante herramientas gráficas sobre el nivel de madurez de la organización frente a lo exigido por la norma COBIT.
- Generación de diversos reportes de control y de resultados de las evaluaciones realizadas.
- Permite la exportación de los diferentes reportes a herramientas como Microsoft Word.

A continuación se presenta gráficamente dicha herramienta:

Figura 5.1. Pantalla de Ingreso de COBIT Advisor

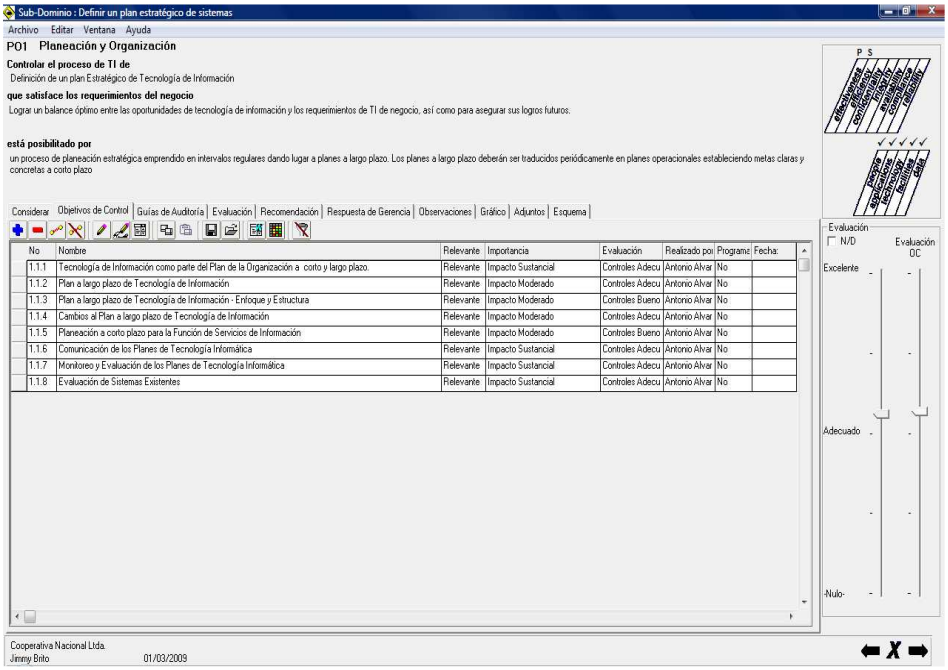


Figura 5.2. Pantalla de Revisión de COBIT Advisor

Una vez que el evaluador ha identificado los dominios y los objetivos de control de COBIT que ha decidido evaluar, puede proceder con la revisión del cumplimiento de dichos lineamientos de forma sencilla, pudiendo observar rápidamente mediante gráficos e informes personalizados y predefinidos los resultados de la evaluación y el nivel de cumplimiento de los procesos de TI frente al estándar COBIT.

5.2. Auditoria en ambientes de procesamiento electrónico de datos, su evolución y aplicación

La Auditoría a través de los años ha ido evolucionando de forma continua a medida que las organizaciones y los procesos dentro de ellas han ido cambiando. El rol del auditor es cada vez más importante dentro de las organizaciones, ya que su misión es ser un asesor para la Alta Dirección en la definición de las políticas, controles y procedimientos para la implementación de un adecuado control interno y un revisor de su efectivo cumplimiento.

En 1949 la AICPA (American Institute of Certified Public Accountants) hizo la siguiente definición: "El control interno comprende el plan de organización, todos los métodos coordinados y las medidas adoptadas en el negocio, para proteger sus activos, verificar la exactitud y confiabilidad de sus datos contables, promover la eficiencia en la operaciones y estimular la adhesión a la prácticas ordenadas por la gerencia".

Como se puede notar de la definición anterior, el control interno abarca a toda la organización desde un punto de vista administrativo, operacional y financiero. En el caso de las COAC's el control interno es el pilar fundamental sobre el cual se basan sus actividades y de ello dependerá su éxito o fracaso en el largo plazo. Es por ello, que la función de auditoría ha tenido que evolucionar acorde con la evolución que ha tenido el control interno en las organizaciones, tal es así que en sus comienzos se basaba en el control y cuadre del efectivo, luego en la revisión y cuadre de los inventarios,

posteriormente en la eficiencia y control operacional y en la actualidad se basa en la evaluación integral de riesgos.

Dado que en la actualidad la tecnología es la base sobre la cual se desarrollan las operaciones de las COAC's y en general de las organizaciones modernas, es necesario disponer de herramientas informáticas que permitan por un lado, analizar el universo de transacciones de la Entidad y por otro lado, poder controlar el trabajo de auditoría. Los auditores disponen de herramientas muy interesantes como ACL e IDEA, para el análisis de datos y de AutoAudit y ProAudit para la planeación y control de la auditoría; entre muchas otras herramientas.

5.2.1. ACL

ACL es una poderosa herramienta para la extracción y análisis de datos que permite la conexión con diferentes tipos de bases de datos y la conversión de archivos de texto y hojas electrónicas, permitiéndole al auditor explorar en forma completa la información transaccional de la Entidad; lo cual, es importante ya que anteriormente cuando no existían este tipo de herramientas el auditor sólo podía tomar muestras para realizar sus pruebas de auditoría. A continuación se presenta la herramienta ACL en forma gráfica:

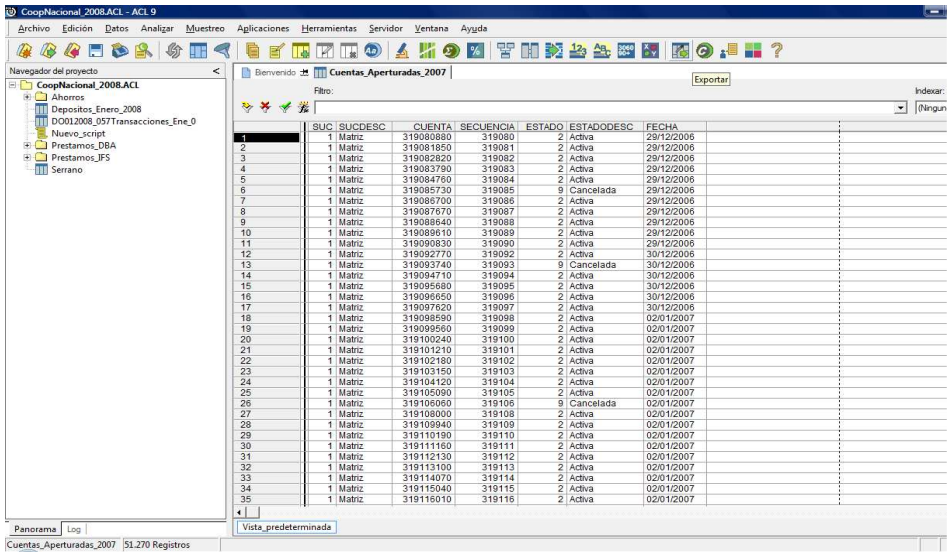


Figura 5.3 Pantalla de exploración de archivos de ACL

El uso de ACL permite entre otras cosas:

- Acceder a cualquier tipo de estructura de datos para su análisis sin el riesgo de que sea alterada o modificada.
- Detectar registros faltantes a través del análisis de secuencias.
- Creación de campos calculados para realizar pruebas de cuadre o totalizaciones.
- Capacidad de filtrar registros de acuerdo a parámetros de consulta.
- Posibilidad de extraer registros y crear nuevas estructuras de datos a partir de ellos para un mejor análisis de la información.
- Creación de programas para la automatización de análisis recurrentes de información.
- Diseño de procesos automáticos de carga de información.
- Reportes y gráficos para la presentación de los resultados del análisis.
- Creación de tablas dinámicas para un mejor modelamiento de la información a ser analizada.
- Posibilidad de realizar análisis estadístico sobre el comportamiento de la información a través del análisis Benford.

5.2.2. AUTOAUDIT

AutoAudit es una herramienta informática para la administración de auditorías basadas en la evaluación del riesgo que le permite al auditor entre otras cosas:

- Planificación de la auditoria por procesos basado en la evaluación integral de los riesgos.
- Asignación de tareas para el equipo de auditoría.
- Manejo de papeles de trabajo de la auditoría realizada y colaboración grupal, para la revisión y aprobación de papeles de

trabajo. Permite ver la trazabilidad de los documentos para posteriores auditorías de los papeles de trabajo.

- Permite la creación de plantillas de papeles de trabajo. El informe de auditoría puede ser previamente diseñado y es capaz de extraer la información de los diversos papeles de trabajo en forma automática.
- Manejo de perfiles por usuarios para el acceso a la herramienta.
- Para las firmas de auditoría les permite asignación de horas y costos de las diferentes etapas de la auditoría para poder establecer los costos totales del trabajo de campo.
- Es posible anexar los informes generados a través de ACL como papeles de trabajo de la auditoría.
- Permite a los auditores externos disponer de sus papeles de trabajo en forma remota y permite su integración posterior.

5.3. Control versus eficiencia: el paradigma de las pistas de auditoría en ambientes de procesamiento electrónico de datos

Dentro de la gestión del riesgo operativo es necesario que una vez que se hayan identificado los diferentes eventos de riesgo y se hayan definido las acciones preventivas, correctivas y de recuperación para cada uno de esos eventos, la Entidad debe crear bases de datos en donde se registren las ocasiones en las que se presentan los eventos, su impacto, las acciones tomadas y demás información de relevancia que permita luego ser analizada y poder determinar aspectos como: la frecuencia y probabilidad de ocurrencia, la eficiencia y eficacia de los controles y las medidas mitigantes para minimizar la ocurrencia futura de tales eventos.

Dicha información es necesaria para que la unidad de Riesgos y la Unidad de Auditoría puedan hacer revisiones periódicas sobre la eficiencia de los controles para mitigar los riesgos y los resultados obtenidos producto de la implementación de la administración del riesgo operativo en la Entidad. Una información oportuna al respecto, mediante dichas pistas de auditoría,

permitirá tomar los correctivos necesarios ya que la administración del riesgo operativo debe estar en evolución y mejora continua.

Dicha Base de Datos de Eventos debe concebir el registro de todos los eventos posibles por cada área o tipo de evento de riesgo; es decir, para Procesos, Personas, Tecnología de Información y Eventos Externos. En el caso de Tecnología de Información, se debe definir los eventos de riesgo por subáreas para un mejor manejo y categorización de dichos eventos. Por ejemplo se puede dividir en:

- Aplicaciones en Producción
- Aplicaciones en Desarrollo
- Redes y Comunicaciones
- Equipos e Infraestructura
- Bases de Datos
- Respaldos y recuperación
- Recepción y Envío de Información Externa
- Help Desk y Soporte técnico, entre otros…

O podría dividirse los eventos por servicios brindados a través del área de tecnología, por ejemplo:

- Servicio de Sistemas de información
- Servicio de Desarrollo y Mantenimiento de Sistemas de Información
- Servicio de Red LAN
- Servicio de Red WAN
- Servicio de Internet
- Servicio de Seguridad Informática
- Servicio de Video vigilancia y CCTV
- Servicio de Mantenimiento de Equipos
- Servicio de Soporte Técnico y Help Desk
- Servicio de Transferencias Interbancarias
- Servicio de Telefonía, entre otros…

Queda a disposición de la Entidad el determinar qué tipo de categorización definir para agrupar sus eventos de riesgos relacionados con la tecnología de información, lo más importante no es la forma sino el hacerlo y cumplir con el registro de los eventos cuando estos se presenten. Este punto hay que recalcarlo debido a que para muchos profesionales de TI les parece ineficiente y hasta molesto tener que registrar los eventos de riesgo ocurridos en sus respectivas áreas de responsabilidad.

Por otro lado, dentro de la gestión del riesgo de la tecnología de información, se debe tener en cuenta la importancia de que los sistemas de información cuenten con suficientes pistas de auditoría para el registro de las actividades o acciones realizadas por los usuarios durante sus sesiones o conexión con la base de datos transaccional; de tal forma que se pueda conocer por cada transacción ingresada, modificada o eliminada, quién la realizó, a qué fecha y hora, desde qué computador y desde qué opción del sistema, entre otras cosas. La idea es disponer de pistas de auditoría útiles y trazables; es decir, que permita conocer los pasos que siguió el Usuario dentro del Sistema de Información al realizar la acción que se está auditando.

Así mismo, tal como deben existir pistas de auditoría para conocer las actividades de los usuarios dentro de los Sistemas de Información, también es necesario que se habiliten las pistas de auditoría nativas de las cuales dispone la base de datos, ya que soluciones como Sybase, Oracle y SQL Server disponen de un sin número de log's o registros de actividad por usuario dentro de la base de datos; lo cual, permite conocer las actividades realizadas por el o los DBA de la Entidad, ya que al disponer de herramientas de administración y acceso a la base de datos fuera del Sistema de Información Institucional, y que cabe señalar muchas veces no están debidamente restringidas ni controladas adecuadamente, podría existir algún tipo de manipulación de la información sin que nadie se dé por enterado hasta cuando las consecuencias sean graves.

Por ello, la Unidad de Riesgos y de Auditoría Interna deben recordar lo siguiente respecto a las bases de datos:

- Deben estar habilitadas las pistas de auditoría inherentes de la base de datos para conocer la actividad del DBA. Las pistas de auditoría de la base de datos deben ser auditadas en forma diaria de ser posible.
- Deben existir pistas de auditoría a nivel de las aplicaciones para conocer la actividad de los usuarios dentro de las sesiones de conexión a la base de datos.
- El DBA no debe disponer de la contraseña del usuario Administrador de la Base de Datos. Dicha clave debe ser conocida sólo por el Jefe de Riesgos o de ser posible por un Oficial de Seguridad Informática. La gerencia general deberá disponer una copia de la clave en sobre sellado.
- Se debe registrar todos los accesos realizados por el usuario Administrador de la Base de Datos y detallar la actividad realizada.

En todos los casos antes mencionados, siempre existirá una contraposición entre el control y la eficiencia, ya que un mayor control significa mayor uso de recursos técnicos y humanos para poder implementarlos. No obstante, los beneficios obtenidos de implementar los controles valen la pena una vez que se determina el grado de disminución del riesgo que podría lograrse; y, aunque esto signifique una dura resistencia por parte de muchos usuarios y funcionarios de la Entidad, con el paso del tiempo será parte integral y normal dentro de sus actividades, por ello, la necesidad de que exista una cultura de responsabilidad y afinidad hacia la administración del riesgo por parte de todos quienes la integran.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones:

- Las Cooperativas de Ahorro y Crédito en el Ecuador en los últimos años han tenido un crecimiento muy importante a nivel financiero y operacional, lo que se ve reflejado en el aumento de los depósitos a la vista y las operaciones de crédito; convirtiéndose después de los bancos, en el principal subsector financiero del País.
- El uso de la tecnología y los sistemas de información en las Cooperativas de Ahorro y Crédito es un aspecto fundamental dentro de la planificación estratégica, la realización de sus operaciones, el control interno y financiero y el mejoramiento de los productos y servicios ofrecidos a sus clientes.
- El Control Interno es una herramienta fundamental para lograr la eficiencia, eficacia, productividad y el desarrollo operativo y administrativo de las COAC's, bajo un ambiente de prevención de riesgos y proactividad en el logro de los objetivos institucionales.
- Las Cooperativas de Ahorro y Crédito tienen la necesidad de adaptar su gestión hacia una cultura de prevención y administración de los diferentes riesgos a los cuales se enfrenta su giro de negocio; entre los que según el Acuerdo de Basilea se componen en riesgo de mercado, riesgo de liquidez y riesgo operacional.
- La Superintendencia de Bancos y Seguros del Ecuador consciente de la necesidad de que las COAC's incorporen a sus procesos de negocio la administración integral de sus riesgos de acuerdo a los lineamientos del Acuerdo de Basilea, ha emitido un conjunto de resoluciones y normativas orientadas hacia una administración de los riesgos, responsable y eficaz en las Entidades Financieras que se encuentran bajo su control.
- La resolución conocida como 834 emitida por la Superintendencia de Bancos incorpora los lineamientos y mejores prácticas de control interno para la administración del riesgo operacional para las Entidades Financieras del Ecuador e identifica 4 aspectos de la

administración del riesgo operacional que deben ser administrados en forma adecuada: los procesos, las personas, la tecnología de información y los eventos externos.

- La administración del riesgo tecnológico es un aspecto fundamental dentro de la gestión de riesgo operativo y es una de las responsabilidades y desafíos más importantes a las cuales se enfrentan las COAC's en el Ecuador, debido a que involucra el uso de recursos organizacionales, humanos, financieros y tecnológicos.
- Existen en la actualidad una serie de lineamientos, estándares y mejores prácticas para una efectiva administración del riesgo, la entrega de servicios y la seguridad relacionada con la tecnología de información, entre los que se encuentran: COBIT, ISO 27001, ITIL, entre otros.
- Es posible dentro de las COAC's crear un marco de control integral para la administración del riesgo tecnológico, basado en las directrices de COSO-ERM, ISO 27001, COBIT y la Resolución 834 que garantice la seguridad de la información, la salvaguarda de los recursos tecnológicos y la continuidad del negocio.
- El rol de auditoría ha evolucionado en los últimos años de tal forma que se ha convertido en un factor importante dentro de la evaluación del riesgo tecnológico y en la mejora continua de los procesos de TI, a través del uso de herramientas tecnológicas para el análisis de las operaciones, la evaluación de riesgos y la planificación de la auditoría.

Recomendaciones

- Las Cooperativas de Ahorro y Crédito deben estar conscientes sobre la necesidad de incorporar a sus procesos de negocio la administración del riesgo operacional y del control interno como una oportunidad para lograr los objetivos institucionales; agregar valor a sus líneas de negocio y estructuras organizacionales; alcanzar una ventaja competitiva frente a la competencia; y, garantizar en forma sustentable su desarrollo administrativo, operativo, financiero y tecnológico.

- Las Cooperativas de Ahorro y Crédito a través de los diferentes marcos de referencia, como COBIT, ITIL, ISO 27000 y la Norma 834, deben adaptar sus lineamientos, políticas y procedimientos de control interno hacia la administración y continuidad de sus procesos de Tecnología de Información, ya que estos últimos, son la base fundamental sobre la que se desarrollan sus operaciones y cuya interrupción pueden generar pérdidas importantes a nivel financiero y reputacional.

- La Administración del riesgo tecnológico permitirá a las COAC's hacer frente a diversos eventos y escenarios de riesgo que pudieran poner en peligro la continuidad operativa del negocio; y para ello, es necesaria la participación de toda la organización y el apoyo fundamental de la Gerencia General en la definición y formalización de las políticas de seguridad y en la implementación de un adecuado control interno de la tecnología de información.

- En el mercado están disponibles diversas herramientas informáticas para la administración del riesgo tecnológico basado en los estándares y mejores prácticas que pueden ser utilizados por los responsables de definir, implementar y controlar el riesgo tecnológico en las COAC's.

APÉNDICE 1. Tabla de Calificación de Riesgos del Sistema Financiero (Fuente: Superintendencia de Bancos)

AAA.- La situación de la institución financiera es muy fuerte y tiene una sobresaliente trayectoria de rentabilidad, lo cual se refleja en una excelente reputación en el medio, muy buen acceso a sus mercados naturales de dinero y claras perspectivas de estabilidad. Si existe debilidad o vulnerabilidad en algún aspecto de las actividades de la institución, ésta se mitiga enteramente con las fortalezas de la organización;

AA.- La institución es muy sólida financieramente, tiene buenos antecedentes de desempeño y no parece tener aspectos débiles que se destaquen. Su perfil general de riesgo, aunque bajo, no es tan favorable como el de las instituciones que se encuentran en la categoría más alta de calificación;

A.- La institución es fuerte, tiene un sólido récord financiero y es bien recibida en sus mercados naturales de dinero. Es posible que existan algunos aspectos débiles, pero es de esperarse que cualquier desviación con respecto a los niveles históricos de desempeño de la entidad sea limitada y que se superará rápidamente. La probabilidad de que se presenten problemas significativos es muy baja, aunque de todos modos ligeramente más alta que en el caso de las instituciones con mayor calificación;

BBB.- Se considera que claramente esta institución tiene buen crédito. Aunque son evidentes algunos obstáculos menores, éstos no son serios y/o son perfectamente manejables a corto plazo;

BB.- La institución goza de un buen crédito en el mercado, sin deficiencias serias, aunque las cifras financieras revelan por lo menos un área fundamental de preocupación que le impide obtener una calificación mayor. Es posible que la entidad haya experimentado un período de dificultades recientemente, pero no se espera que esas presiones perduren a largo plazo. La capacidad de la institución para afrontar imprevistos, sin embargo, es menor que la de organizaciones con mejores antecedentes operativos:

B.- Aunque esta escala todavía se considera como crédito aceptable, la institución tiene algunas deficiencias significativas. Su capacidad para manejar un mayor deterioro está por debajo de las instituciones con mejor calificación;

C.- Las cifras financieras de la institución sugieren obvias deficiencias, muy probablemente relacionadas con la calidad de los activos y/o de una mala estructuración del balance. Hacia el futuro existe un considerable nivel de incertidumbre. Es dudosa su capacidad para soportar problemas inesperados adicionales;

D.- La institución tiene considerables deficiencias que probablemente incluyen dificultades de fondeo o de liquidez. Existe un alto nivel de incertidumbre sobre si esta institución podrá afrontar problemas adicionales;

E.- la institución afronta problemas muy serios y por lo tanto existe duda sobre si podrá continuar siendo viable sin alguna forma de ayuda externa, o de otra naturaleza.

A las categorías descritas se pueden asignar los signos (+) o (-) para indicar su posición relativa dentro de la respectiva categoría.

APÉNDICE 2. Resolución No JB-2005-834 emitida por la Superintendencia de Bancos y Seguros

LIBRO I.- 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)

SECCIÓN I.- ÁMBITO, DEFINICIONES Y ALCANCE

ARTÍCULO 1.- Las disposiciones de la presente 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, a las cuales, en el texto de este capítulo se las denominará como instituciones controladas.

Para efecto de administrar adecuadamente el riesgo operativo, además de las disposiciones contenidas en el capítulo I "De la gestión integral y control de riesgos", las instituciones controladas observarán las disposiciones del presente capítulo.

ARTÍCULO 2.- Para efectos de la aplicación de las disposiciones del presente capítulo, se considerarán las siguientes definiciones:

2.1 Alta gerencia.- La integran los presidentes y vicepresidentes ejecutivos, gerentes generales, vicepresidentes o gerentes departamentales, entre otros, responsables de ejecutar las disposiciones del directorio u organismo que haga sus veces, quienes toman decisiones de alto nivel, de acuerdo con las funciones asignadas y la estructura organizacional definida en cada institución controlada;

2.2 Evento de riesgo operativo.- Es el hecho que puede derivar en pérdidas financieras para la institución controlada;

2.3 Factor de riesgo operativo.- Es la causa primaria o el origen de un evento de riesgo operativo. Los factores son los procesos, personas, tecnología de información y eventos externos;

2.4 Proceso.- Es el conjunto de actividades que transforman insumos en productos o servicios con valor para el cliente, sea interno o externo;

2.5 Insumo.- Es el conjunto de materiales, datos o información que sirven como entrada a un proceso;

2.6 Proceso crítico.- Es el indispensable para la continuidad del negocio y las operaciones de la institución controlada, y cuya falta de identificación o aplicación deficiente puede generarle un impacto financiero negativo;

2.7 Actividad.- Es el conjunto de tareas;

2.8 Tarea.- Es el conjunto de pasos o procedimientos que conducen a un resultado final visible y mesurable;

2.9 Procedimiento.- Es el método que especifica los pasos a seguir para cumplir un propósito determinado;

2.10 Línea de negocio.- Es una especialización del negocio que agrupa procesos encaminados a generar productos y servicios especializados para atender un segmento del mercado objetivo definido en la planificación estratégica de la entidad;

2.11 Datos.- Es cualquier forma de registro electrónico, óptico, magnético, impreso o en otros medios, susceptible de ser capturado, almacenado, procesado y distribuido;

2.12 Información.- Es cualquier forma de registro electrónico, óptico, magnético o en otros medios, previamente procesado a partir de datos, que puede ser almacenado, distribuido y sirve para análisis, estudios y toma de decisiones;

2.13 Información crítica.- Es la información considerada esencial para la continuidad del negocio y para la adecuada toma de decisiones;

2.14 Administración de la información.- Es el proceso mediante el cual se captura, procesa, almacena y transmite información, independientemente del medio que se utilice; ya sea impreso, escrito en papel, almacenado electrónicamente, transmitido por correo o por medios electrónicos o presentado en imágenes;

2.15 Tecnología de información.- Es el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, servicios asociados, entre otros;

2.16 Aplicación.- Se refiere a los procedimientos programados a través de alguna herramienta tecnológica, que permiten la administración de la información y la oportuna toma de decisiones;

2.17 Instalaciones.- Es la infraestructura que permite alojar los recursos físicos relacionados con la tecnología de información;

2.18 Responsable de la información.- Es la persona encargada de identificar y definir claramente los diversos recursos y procesos de seguridad lógica relacionados con las aplicaciones;

2.19 Seguridad de la información.- Son los mecanismos implantados que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella;

2.20 Seguridades lógicas.- Se refieren a la seguridad en el uso del software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información;

2.21 Confidencialidad.- Es la garantía de que sólo el personal autorizado accede a la información preestablecida;

2.22 Integridad.- Es la garantía de mantener la totalidad y exactitud de la información y de los métodos de procesamiento;

2.23 Disponibilidad.- Es la garantía de que los usuarios autorizados tienen acceso a la información cada vez que lo requieran a través de los medios adecuados que satisfagan sus necesidades;

2.24 Cumplimiento.- Se refiere a la observancia de las leyes, regulaciones y acuerdos contractuales a los que los procesos de las instituciones controladas están sujetos;

2.25 Pista de auditoría.- Es el registro de datos lógicos de las acciones o sucesos ocurridos en los sistemas aplicativos u operativos, con el propósito de mantener información histórica para fines de control, supervisión y auditoría;

2.26 Medios electrónicos.- Son los elementos de la tecnología que tienen características digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares;

2.27 Transferencia electrónica de información.- Es la forma de enviar, recibir o transferir en forma electrónica datos, información, archivos, mensajes, entre otros;

2.28 Encriptación.- Es el proceso mediante el cual la información o archivos son alterados en forma lógica, con el objetivo de evitar que alguien no autorizado pueda interpretarlos al verlos o copiarlos, por lo que se utiliza una clave en el origen y en el destino;

2.29 Plan de continuidad.- Está orientado a asegurar la continuidad del negocio, la satisfacción del cliente y la productividad a pesar de eventos inesperados. Se ejecuta permanentemente como parte de la administración de riesgos tanto en la información como en la operación. Un plan de continuidad incluye un plan de contingencia, un plan de reanudación y un plan de recuperación;

2.30 Plan de contingencia.- Es el conjunto de procedimientos alternativos a la operatividad normal de la entidad cuya finalidad es la de permitir su funcionamiento, buscando minimizar el impacto financiero que pueda ocasionar cualquier evento inesperado específico. El plan de contingencia se ejecuta el momento en que se produce dicho evento;

2.31 Plan de reanudación.- Especifica los procesos y recursos para mantener la continuidad de las operaciones en la misma ubicación del problema;

2.32 Plan de recuperación.- Especifica los procesos y recursos para recuperar las funciones del negocio en una ubicación alterna dentro o fuera de la institución;

2.33 Eficacia.- Es la capacidad para contribuir al logro de los objetivos institucionales de conformidad con los parámetros establecidos;

2.34 Eficiencia.- Es la capacidad para aprovechar racionalmente los recursos disponibles en pro del logro de los objetivos institucionales, procurando la optimización de aquellos y evitando dispendios y errores; y,

2.35 Riesgo legal.- Es la probabilidad de que una institución del sistema financiero sufra pérdidas directas o indirectas; de que sus activos se encuentren expuestos a situaciones de mayor vulnerabilidad; de que sus pasivos y contingentes puedan verse incrementados más allá de los niveles esperados, o de que el desarrollo de sus operaciones enfrente la eventualidad de ser afectado negativamente, debido a error, negligencia, impericia, imprudencia o dolo, que deriven de la inobservancia, incorrecta o inoportuna aplicación de disposiciones legales o normativas, así como de instrucciones de carácter general o particular emanadas de los organismos de control, dentro de sus respectivas competencias; o, en sentencias o resoluciones jurisdiccionales o administrativas adversas; o de la deficiente redacción de los textos, formalización o ejecución de actos, contratos o transacciones, inclusive distintos a los de su giro ordinario de negocio, o porque los derechos de las partes contratantes no han sido claramente estipuladas. (sustituido con resolución No. JB-2008-1202 de 23 de octubre del 2008) De acuerdo con lo dispuesto en el numeral 2 del artículo 18 del Código Civil, los términos utilizados en la definición de riesgo legal se entenderán en su sentido natural y obvio, según el uso general de las mismas palabras, a menos de que tengan definiciones diferentes expresadas en la ley, reglamentos y demás normativa. (incluido con resolución No. JB- 2008-1202 de 23 de octubre del 2008)

ARTÍCULO 3.- Para efectos del presente capítulo, el riesgo operativo se entenderá como la posibilidad de que se ocasionen pérdidas financieras por eventos derivados de fallas o insuficiencias en los procesos, personas, tecnología de información y por eventos externos.

El riesgo operativo incluye el riesgo legal en los términos establecidos en el numeral 2.35 del artículo 2.

El riesgo operativo no trata sobre la posibilidad de pérdidas originadas en cambios inesperados en el entorno político, económico y social.

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,:

4.1 Procesos.- Con el objeto de 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, que deberán ser agrupados de la siguiente manera:

4.1.1 Procesos gobernantes o estratégicos.- Se considerarán a aquellos que proporcionan directrices a los demás procesos y son realizados por el directorio u organismo que haga sus veces y por la alta gerencia para poder cumplir con los objetivos y políticas institucionales. Se refieren a la planificación estratégica, los lineamientos de acción básicos, la estructura organizacional, la administración integral de riesgos, entre otros;

4.1.2 Procesos productivos, fundamentales u operativos.- Son los procesos esenciales de la entidad destinados a llevar a cabo las actividades que permitan ejecutar efectivamente las políticas y estrategias relacionadas con la calidad de los productos o servicios que ofrecen a sus clientes; y,

4.1.3 Procesos habilitantes, de soporte o apoyo.- Son aquellos que apoyan a los procesos gobernantes y productivos, se encargan de proporcionar personal competente, reducir los riesgos del trabajo, preservar la calidad de los materiales, equipos y herramientas, mantener las condiciones de operatividad y funcionamiento, coordinar y controlar la eficacia del desempeño administrativo y la optimización de los recursos. Identificados los procesos críticos, se implantarán mecanismos o alternativas que ayuden a la entidad a evitar incurrir en pérdidas o poner en riesgo la continuidad del negocio y sus operaciones. Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas para un adecuado diseño, control, actualización y seguimiento de los procesos.

Las políticas deben referirse por lo menos a: (i) diseño claro de los procesos, los cuales deben ser adaptables y dinámicos; (ii) descripción en secuencia lógica y ordenada de las actividades, tareas, y controles; (iii) determinación de los responsables de los procesos, que serán aquellas personas encargadas de su correcto funcionamiento, a través de establecer medidas y fijar objetivos para gestionarlos y mejorarlos, garantizar que las metas globales se cumplan, definir los límites y alcance, mantener contacto con los clientes internos y externos del proceso para garantizar que se satisfagan y se conozcan sus expectativas, entre otros; (iv) difusión y comunicación de los procesos buscando garantizar su total aplicación; y, (v) actualización y mejora continua a través del seguimiento permanente en su aplicación.

Deberá existir una adecuada separación de funciones que evite concentraciones de carácter incompatible, entendidas éstas como aquellas tareas cuya combinación en las competencias de una sola persona, eventualmente, podría permitir la realización o el ocultamiento de fraudes, errores, omisiones u otros eventos de riesgo operativo.

Las instituciones controladas deberán mantener inventarios actualizados de los procesos existentes, que cuenten, como mínimo con la siguiente información: tipo de proceso (gobernante, productivo y de apoyo), nombre del proceso, responsable, productos y

servicios que genera el proceso, clientes internos y externos, fecha de aprobación, fecha de actualización, además de señalar si se trata de un proceso crítico.

4.2 Personas.- Las instituciones controladas deben administrar el capital humano 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.

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 apropiada planificación y administración del capital humano, los cuales considerarán los procesos de incorporación, permanencia y desvinculación del personal al servicio de la institución.

Dichos procesos corresponden a:

4.2.1 Los procesos de incorporación.- Que comprenden la planificación de necesidades, el reclutamiento, la selección, la contratación e inducción de nuevo personal;

4.2.2 Los procesos de permanencia.- Que cubren la creación de condiciones laborales idóneas; la promoción de actividades de capacitación y formación que permitan al personal aumentar y perfeccionar sus conocimientos, competencias y destrezas; la existencia de un sistema de evaluación del desempeño; desarrollo de carrera; rendición de cuentas; e incentivos que motiven la adhesión a los valores y controles institucionales; y,

4.2.3 Los procesos de desvinculación.- Que comprenden la planificación de la salida del personal por causas regulares, preparación de aspectos jurídicos para llegar al finiquito y la finalización de la relación laboral.

Los procesos de incorporación, permanencia y desvinculación antes indicados deberán ser soportados técnicamente, ajustados a las disposiciones legales y transparentes para garantizar condiciones laborales idóneas.

Las instituciones controladas deberán analizar su organización con el objeto de evaluar si han definido el personal necesario y las competencias idóneas para el desempeño de cada puesto, considerando no sólo experiencia profesional, formación académica, sino también los valores, actitudes y habilidades personales que puedan servir como criterio para garantizar la excelencia institucional.

Las instituciones controladas mantendrán información actualizada del capital humano, que permita una adecuada toma de decisiones por parte de los niveles directivos y la realización de análisis cualitativos y cuantitativos de acuerdo con sus necesidades.

Dicha información deberá referirse al personal existente en la institución; a la formación académica y experiencia; a la forma y fechas de selección, reclutamiento y contratación; información histórica sobre los eventos de capacitación en los que han participado; cargos que han desempeñado en la institución; resultados de evaluaciones realizadas; fechas y causas de separación del personal que se ha desvinculado de la institución; y, otra información que la institución controlada considere pertinente.

4.3 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.

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:

4.3.1.1 El apoyo y compromiso formal del directorio u organismo que haga sus veces y la alta gerencia;

4.3.1.2 Un plan funcional de tecnología de información alineado con el plan estratégico institucional; y, un plan operativo que establezca las actividades a ejecutar en el corto plazo (un año), de manera que se asegure el logro de los objetivos institucionales propuestos;

4.3.1.3 Tecnología de información acorde a las operaciones del negocio y al volumen de transacciones, monitoreada y proyectada según las necesidades y crecimiento de la institución;

4.3.1.4 Un responsable de la información que se encargue principalmente de definir y autorizar de manera formal los accesos y cambios funcionales a las aplicaciones y monitorear el cumplimiento de los controles establecidos;

4.3.1.5 Políticas, procesos y procedimientos de tecnología de información definidos bajo estándares de general aceptación que garanticen la ejecución de los criterios de control interno de eficacia, eficiencia y cumplimiento, debidamente aprobados por el directorio u organismo que haga sus veces, alineados a los objetivos y actividades de la institución;

4.3.1.6 Difusión y comunicación a todo el personal involucrado de las mencionadas políticas, procesos y procedimientos, de tal forma que se asegure su implementación; y,

4.3.1.7 Capacitación y entrenamiento técnico al personal del área de tecnología de información y de los usuarios de la misma.

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:

4.3.2.1 Manuales o reglamentos internos, debidamente aprobados por el directorio u organismo que haga sus veces, que establezcan como mínimo las responsabilidades y procedimientos para la operación, el uso de las instalaciones de procesamiento de información y respuestas a incidentes de tecnología de información;

4.3.2.2 Un procedimiento de clasificación y control de activos de tecnología de información, que considere por lo menos, su registro e identificación, así como los responsables de su uso y mantenimiento, especialmente de los más importantes;

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, las instituciones controladas deben contar al menos con lo siguiente:

4.3.3.1 Requerimientos contractuales convenidos que definan la propiedad de la información y de las aplicaciones; y, la responsabilidad de la empresa proveedora de la tecnología en caso de ser vulnerables sus sistemas, a fin de mantener la integridad, disponibilidad y confidencialidad de la información; y,

4.3.3.2 Requerimientos contractuales convenidos que establezcan que las aplicaciones sean parametrizables, que exista una transferencia del conocimiento y que se entregue documentación técnica y de usuario, a fin de reducir la dependencia de las instituciones controladas con proveedores externos y los eventos de riesgo operativo que esto origina.

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:

4.3.4.1 Políticas y procedimientos de seguridad de la información que establezcan sus objetivos, importancia, normas, principios, requisitos de cumplimiento, responsabilidades y comunicación de los incidentes relativos a la seguridad; considerando los aspectos legales, así como las consecuencias de violación de estas políticas;

4.3.4.2 La identificación de los requerimientos de seguridad relacionados con la tecnología de información, considerando principalmente: la evaluación de los riesgos que enfrenta la institución; los requisitos legales, normativos, reglamentarios y contractuales; y, el conjunto específico de principios, objetivos y condiciones para el procesamiento de la información que respalda sus operaciones;

4.3.4.3 Los controles necesarios para asegurar la integridad, disponibilidad y confidencialidad de la información administrada;

4.3.4.4 Un sistema de administración de las seguridades de acceso a la información, que defina las facultades y atributos de los usuarios, desde el registro, eliminación y modificación, pistas de auditoría; además de los controles necesarios que permitan verificar su cumplimiento en todos los ambientes de procesamiento;

4.3.4.5 Niveles de autorización de accesos y ejecución de las funciones de procesamiento de las aplicaciones, formalmente establecidos, que garanticen una adecuada segregación de funciones y reduzcan el riesgo de error o fraude;

4.3.4.6 Adecuados sistemas de control y autenticación para evitar accesos no autorizados, inclusive de terceros; y, ataques externos especialmente a la información crítica y a las instalaciones de procesamiento;

4.3.4.7 Controles adecuados para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia, así como instalar y actualizar periódicamente aplicaciones de detección y desinfección de virus informáticos y demás software maliciosos;

4.3.4.8 Controles formales para proteger la información contenida en documentos; medios de almacenamiento u otros dispositivos externos; el uso e intercambio electrónico de datos contra daño, robo, accesos, utilización o divulgación no autorizada de información para fines contrarios a los intereses de la entidad, por parte de todo su personal y de sus proveedores;

4.3.4.9 Instalaciones de procesamiento de información crítica en áreas protegidas con los suficientes controles que eviten el acceso de personal no autorizado y daños a los equipos de computación y a la información en ellos procesada, almacenada o distribuida;

4.3.4.10 Las condiciones físicas y ambientales necesarias para garantizar el correcto funcionamiento del entorno de la infraestructura de tecnología de información;

4.3.4.11 Un plan para evaluar el desempeño del sistema de administración de la seguridad de la información, que permita tomar acciones orientadas a mejorarlo; y,

4.3.4.12 Las instituciones controladas que ofrezcan los servicios de transferencias y transacciones electrónicas deberán contar con políticas y procedimientos de seguridad de la información que garanticen que las operaciones sólo pueden ser realizadas por

personas debidamente autorizadas; que el canal de comunicaciones utilizado sea seguro, mediante técnicas de encriptación de información; que existan mecanismos alternos que garanticen la continuidad del servicio ofrecido; y, que aseguren la existencia de pistas de auditoría.

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

4.3.5.1 Controles para minimizar riesgos potenciales de sus equipos de computación ante eventos imprevistos, tales como: fallas, daños o insuficiencia de los recursos de tecnología de información; robo; incendio; humo; inundaciones; polvo; interrupciones en el fluido eléctrico, desastres naturales; entre otros;

4.3.5.2 Políticas y procedimientos de respaldo de información periódicos, que aseguren al menos que la información crítica pueda ser recuperada en caso de falla de la tecnología de información o con posterioridad a un evento inesperado;

4.3.5.3 Mantener los sistemas de comunicación y redundancia de los mismos que permitan garantizar la continuidad de sus servicios; y,

4.3.5.4 Información de respaldo y procedimientos de restauración en una ubicación remota, a una distancia adecuada que garantice su disponibilidad ante eventos de desastre en el centro principal de procesamiento.

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:

4.3.6.1 Una metodología que permita la adecuada administración y control del proceso de compra de software y del ciclo de vida de desarrollo y mantenimiento de aplicaciones, con la aceptación de los usuarios involucrados;

4.3.6.2 Documentación técnica y de usuario permanentemente actualizada de las aplicaciones de la institución;

4.3.6.3 Controles que permitan asegurar la adecuada administración de versiones de las aplicaciones puestas en producción; y,

4.3.6.4 Controles que permitan asegurar que la calidad de la información sometida a migración, cumple con las características de integridad, disponibilidad y confidencialidad.

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.

4.4 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.

SECCIÓN III.- ADMINISTRACIÓN DEL RIESGO OPERATIVO

ARTÍCULO 5.- En el marco de la administración integral de riesgos, establecido en la sección II “Administración de riesgos”, del capítulo I “De la gestión integral y control de riesgos”, las instituciones controladas incluirán el proceso para administrar el riesgo operativo como un riesgo específico, el cual, si no es administrado adecuadamente puede afectar el logro de los objetivos de estabilidad a largo plazo y la continuidad del negocio.

El diseño del proceso de administración de riesgo operativo deberá permitir a las instituciones controladas identificar, medir, controlar/mitigar y monitorear sus exposiciones a este riesgo al que se encuentran expuestas en el desarrollo de sus negocios y operaciones. Cada institución desarrollará sus propias técnicas o esquemas de administración, considerando su objeto social, tamaño, naturaleza, complejidad y demás características propias.

ARTÍCULO 6.- Para una adecuada administración del riesgo operativo las instituciones controladas deberán cumplir las disposiciones del artículo 4 del presente capítulo y adicionalmente, deberán contar con códigos de ética y de conducta formalmente establecidos; con la supervisión del directorio u organismo que haga sus veces y de la alta gerencia; con una sólida cultura de control interno; con planes de contingencias y de continuidad del negocio debidamente probados; y, con la tecnología de información adecuada.

ARTÍCULO 7.- Con la finalidad de que las instituciones controladas administren adecuadamente el riesgo operativo es necesario que agrupen sus procesos por líneas de negocio, de acuerdo con una metodología establecida de manera formal y por escrito, para lo cual deberán observar los siguientes lineamientos:

7.1 Los procesos productivos deberán asignarse a las líneas de negocio de acuerdo con los productos y servicios que generan, de forma que a cada uno de los procesos le corresponda una sola línea de negocio y que ningún proceso permanezca sin asignar; y,

7.2 Las líneas de negocio también deberán agrupar los procesos gobernantes y los procesos habilitantes que intervienen en las mismas. Si algún proceso gobernante o proceso habilitante interviene en más de una línea de negocio, la entidad deberá utilizar un criterio de asignación objetivo.

ARTÍCULO 8.- Las instituciones controladas deberán identificar, por línea de negocio, los eventos de riesgo operativo, agrupados por tipo de evento, y, las fallas o insuficiencias en los procesos, las personas, la tecnología de información y los eventos externos.

Los tipos de eventos son los siguientes:

8.1 Fraude interno;
8.2 Fraude externo;
8.3 Prácticas laborales y seguridad del ambiente de trabajo;
8.4 Prácticas relacionadas con los clientes, los productos y el negocio;
8.5 Daños a los activos físicos;
8.6 Interrupción del negocio por fallas en la tecnología de información; y,
8.7 Deficiencias en la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros.

En el anexo No. 1 se incluyen algunos casos de eventos de riesgo operativo, agrupados por tipo de evento, fallas o insuficiencias que podrían presentarse en las instituciones controladas y su relación con los factores de riesgo operativo.

Los eventos de riesgo operativo y las fallas o insuficiencias serán identificados en relación con los factores de este riesgo a través de una metodología formal, debidamente documentada y aprobada. Dicha metodología podrá incorporar la utilización de las herramientas que más se ajusten a las necesidades de la institución, entre las cuales podrían estar: autoevaluación, mapas de riesgos, indicadores, tablas de control (scorecards), bases de datos u otras.

ARTICULO 9.- Dentro del proceso de identificación al que se refiere el artículo anterior, las instituciones deben adicionalmente determinar de manera puntual las fallas o insuficiencias de orden legal, de tal manera que les proporcione una visión clara sobre su exposición al riesgo legal, debiendo tener como referencia para el efecto los tipos de evento de riesgo operativo indicados en dicho artículo.

Las fallas o insuficiencias de orden legal deben ser establecidas por las instituciones de acuerdo con su propia percepción y perfil de riesgos, pero deben enfocar por lo menos los siguientes campos: actos societarios; gestión de crédito; operaciones del giro financiero; actividades complementarias no financieras; y, cumplimiento legal y normativo, entendiéndolos dentro de las siguientes conceptualizaciones:

9.1 Actos societarios.- Son todos aquellos procesos jurídicos que debe realizar la institución en orden a ejecutar y perfeccionar las decisiones de la junta general de accionistas o asamblea general de socios o representantes, según sea del caso, y del directorio o cuerpo colegiado que haga sus veces, necesarios para el desenvolvimiento societario de la institución del sistema financiero, atenta su naturaleza jurídica;

9.2 Gestión de crédito.- Es el conjunto de actividades que debe ejecutar la institución del sistema financiero relacionadas con el otorgamiento de operaciones crediticias. Se inicia con la recepción de la solicitud de crédito y termina con la recuperación del valor prestado, sus intereses y comisiones. Incluye la gestión de recuperación de cartera tanto judicial como extrajudicial, la misma que debe proseguir aún cuando la operación crediticia hubiere sido castigada;

9.3 Operaciones del giro financiero.- Es el conjunto de actividades o procesos que realiza la institución del sistema financiero para la ejecución de operaciones propias del giro financiero, distintas a la gestión de crédito;

9.4 Actividades complementarias de las operaciones del giro financiero.- Es el conjunto de actividades o procesos que debe ejecutar la institución del sistema financiero que sin ser propias del giro financiero, son necesarias para el cumplimiento y desarrollo de su objeto social; y,

9.5 Cumplimiento legal y normativo.- Es el proceso mediante el cual la institución del sistema financiero controla que sus actividades y sus operaciones se ajusten a las disposiciones legales y normativas vigentes, así como la capacidad de adecuarse rápida y efectivamente a nuevas disposiciones legales y normativas. (artículo incluido con resolución No. JB-2008-1202 de 23 de octubre del 2008)

ARTÍCULO 10.- Una vez identificados los eventos de riesgo operativo y las fallas o insuficiencias en relación con los factores de este riesgo y su incidencia para la institución, los niveles directivos están en capacidad de decidir si el riesgo se debe asumir, compartirlo, evitarlo o transferirlo, reduciendo sus consecuencias y efectos.

La identificación antes indicada permitirá al directorio u organismo que haga sus veces y a la alta gerencia de la entidad contar con una visión clara de la importancia relativa de los diferentes tipos de exposición al riesgo operativo y su prioridad, con el objeto de alertarlos en la toma de decisiones y acciones, que entre otras, pueden ser: revisar estrategias y políticas; actualizar o modificar procesos y procedimientos establecidos; implantar o modificar límites de riesgo; constituir, incrementar o modificar controles; implantar planes de contingencias y de continuidad del negocio; revisar términos de pólizas de seguro contratadas; contratar servicios provistos por terceros; u otros, según corresponda. (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

ARTÍCULO 11.- En razón de que la administración del riesgo operativo constituye un proceso continuo y permanente, será necesario que adicionalmente las instituciones controladas conformen bases de datos centralizadas, suficientes y de calidad, que permitan registrar, ordenar, clasificar y disponer de información sobre los eventos de riesgo operativo; fallas o insuficiencias incluidas las de orden legal; y, factores de riesgo operativo clasificados por línea de negocio, determinando la frecuencia con que se repite cada evento y el efecto cuantitativo de pérdida producida y otra información que las instituciones controladas consideren necesaria y oportuna, para que a futuro se pueda estimar las pérdidas esperadas e inesperadas atribuibles a este riesgo. (artículo renumerado y reformado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

ARTÍCULO 12.- Aspecto importante de la administración del riesgo operativo es el control, el cual requerirá que las instituciones controladas cuenten con sistemas de control interno adecuados, esto es, políticas, procesos, procedimientos y niveles de control formalmente establecidos y validados periódicamente. Los controles deben formar parte integral de las actividades regulares de la entidad para generar respuestas oportunas ante diversos eventos de riesgo operativo y las fallas o insuficiencias que los ocasionaron. (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

ARTÍCULO 13.- El esquema de administración del riesgo operativo de las instituciones controladas debe estar sujeto a una auditoría interna efectiva e integral, por parte de personal competente, debidamente capacitado y operativamente independiente.

La función de auditoría interna coadyuva al mejoramiento de la efectividad de la administración de riesgos a través de una evaluación periódica, pero no es directamente responsable de la gestión del riesgo operativo. (artículo renumerado con resolución No. JB- 2008-1202 de 23 de octubre del 2008)

ARTÍCULO 14.- Las instituciones controladas deben contar permanentemente con un esquema organizado de reportes que permitan disponer de información suficiente y adecuada para gestionar el riesgo operativo en forma continua y oportuna. (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)
Los reportes deberán contener al menos lo siguiente:

14.1 Detalle de los eventos de riesgo operativo, agrupados por tipo de evento; las fallas o insuficiencias que los originaron relacionados con los factores de riesgo operativo y clasificados por líneas de negocio;

14.2 Informes de evaluación del grado de cumplimiento de las políticas relacionadas con los factores de riesgo operativo y los procesos y procedimientos establecidos por la institución; y,

14.3 Indicadores de gestión que permitan evaluar la eficiencia y eficacia de las políticas, procesos y procedimientos aplicados.

Estos informes deben ser dirigidos a los niveles adecuados de la institución de manera que puedan ser analizados con una perspectiva de mejora constante del desempeño en la administración del riesgo operativo; así como para establecer o modificar políticas, procesos, procedimientos, entre otros.

SECCIÓN IV.- CONTINUIDAD DEL NEGOCIO

ARTÍCULO 15.- Las instituciones controladas deben implementar planes de contingencia y de continuidad, a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción severa del negocio. (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

Para el efecto, deberán efectuar adecuados estudios de riesgos y balancear el costo de la implementación de un plan de continuidad con el riesgo de no tenerlo, esto dependerá de la criticidad de cada proceso de la entidad; para aquellos de muy alta criticidad se deberá implementar un plan de continuidad, para otros, bastará con un plan de contingencia.
Las instituciones controladas deberán establecer un proceso de administración de la continuidad de los negocios, que comprenda los siguientes aspectos claves:

15.1 Definición de una estrategia de continuidad de los negocios en línea con los objetivos institucionales;

15.2 Identificación de los procesos críticos del negocio, aún en los provistos por terceros;

15.3 Identificación de los riesgos por fallas en la tecnología de información;

15.4 Análisis que identifique los principales escenarios de contingencia tomando en cuenta el impacto y la probabilidad de que sucedan;

15.5 Evaluación de los riesgos para determinar el impacto en términos de magnitud de daños, el período de recuperación y tiempos máximos de interrupción que puedan ocasionar los siniestros;

15.6 Elaboración del plan de continuidad del negocio para someterlo a la aprobación del directorio u organismo que haga sus veces;

15.7 Realización de pruebas periódicas del plan y los procesos implantados que permitan comprobar su aplicabilidad y realizar los ajustes necesarios; y,

15.8 Incorporación del proceso de administración del plan de continuidad del negocio al proceso de administración integral de riesgos.

ARTÍCULO 16.- Los planes de contingencia y de continuidad de los negocios deben comprender las previsiones para la reanudación y recuperación de las operaciones. (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

Los planes de contingencia y de continuidad deberán incluir, al menos, lo siguiente:

16.1 Las personas responsables de ejecutar cada actividad y la información (direcciones, teléfonos, correos electrónicos, entre otros) necesaria para contactarlos oportunamente;

16.2 Acciones a ejecutar antes, durante y una vez ocurrido el incidente que ponga en peligro la operatividad de la institución;

16.3 Acciones a realizar para trasladar las actividades de la institución a ubicaciones transitorias alternativas y para el restablecimiento de los negocios de manera urgente;

16.4 Cronograma y procedimientos de prueba y mantenimiento del plan; y,

16.5 Procedimientos de difusión, comunicación y concienciación del plan y su cumplimiento.

SECCIÓN V.- RESPONSABILIDADES EN LA ADMINISTRACIÓN DEL RIESGO OPERATIVO

ARTÍCULO 17.- Las responsabilidades del directorio u organismo que haga sus veces, en cuanto a la administración del riesgo operativo, se regirán por lo dispuesto en la sección III "Responsabilidad en la administración de riesgos", del capítulo I "De la gestión integral y control de riesgos". (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)
Adicionalmente, el directorio u organismo que haga sus veces tendrá las siguientes responsabilidades en relación con la administración del riesgo operativo:

17.1 Crear una cultura organizacional con principios y valores de comportamiento ético que priorice la gestión eficaz del riesgo operativo;

17.2 Aprobar las disposiciones relativas a los procesos establecidos en el numeral 4.1 del artículo 4;

17.3 Aprobar las políticas, procesos y procedimientos para la administración del capital humano conforme con los lineamientos establecidos en el numeral 4.2 del artículo 4;

17.4 Aprobar las políticas y procedimientos de tecnología de información establecidos en el numeral 4.3 del artículo 4; y,

17.5 Aprobar los planes de contingencia y de continuidad del negocio a los que se refiere la sección IV de este capítulo.

ARTÍCULO 18.- Las funciones y responsabilidades del comité de administración integral de riesgos se regirán por lo dispuesto en la sección III "Responsabilidad en la administración del riesgos", del capítulo I "De la gestión integral y control de riesgos". (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)
Adicionalmente, el comité de administración integral de riesgos tendrán las siguientes responsabilidades en relación con la administración del riesgo operativo:

18.1 Evaluar y proponer al directorio u organismo que haga sus veces las políticas y el proceso de administración del riesgo operativo y asegurarse que sean implementados en toda la institución y que todos los niveles del personal entiendan sus responsabilidades con relación al riesgo operativo;

18.2 Evaluar las políticas y procedimientos de procesos, personas y tecnología de información y someterlas a aprobación del directorio u organismo que haga sus veces;

18.3 Definir los mecanismos para monitorear y evaluar los cambios significativos y la exposición a riesgos;

18.4 Evaluar y someter a aprobación del directorio u organismo que haga sus veces los planes de contingencia y de continuidad del negocio a los que se refiere la sección IV del este capítulo; asegurar la aplicabilidad; y, cumplimiento de los mismos; y,

18.5 Analizar y aprobar la designación de líderes encargados de llevar a cabo las actividades previstas en el plan de contingencia y de continuidad del negocio.

ARTICULO 19.- Las funciones y responsabilidades de la unidad de riesgos se regirán por lo dispuesto en la sección III "Responsabilidad en la administración del riesgos", del capítulo I "De la gestión integral y control de riesgos". (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)
Adicionalmente, la unidad de riesgos tendrán las siguientes responsabilidades en relación con la administración del riesgo operativo:

19.1 Diseñar las políticas y el proceso de administración del riesgo operativo;

19.2 Monitorear y evaluar los cambios significativos y la exposición a riesgos provenientes de los procesos, las personas, la tecnología de información y los eventos externos;

19.3 Analizar las políticas y procedimientos propuestos por el área respectiva, para los procesos, personas, eventos externos y tecnología de información, especialmente aquellas relacionadas con la seguridad de la información; (sustituido con resolución No. JB-2008-1202 de 23 de octubre del 2008)

19.4 Liderar el desarrollo, la aplicabilidad y cumplimiento de los planes de contingencia y de continuidad del negocio, al que se refiere la sección IV de este capítulo; así como proponer los líderes de las áreas que deban cubrir el plan de contingencias y de continuidad del negocio; y, (reformado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

19.5 Analizar, monitorear y evaluar los procedimientos de orden legal de la institución; y, en coordinación con las áreas legales, emitir informes que determinen su real exposición al riesgo legal, los cuales deben ser puestos en conocimiento del comité de administración integral de riesgos. (incluido con resolución No. JB-2008-1202 de 23 de octubre del 2008)

SECCIÓN VI.- DISPOSICIONES GENERALES

ARTÍCULO 20.- Para mantener un adecuado control de los servicios provistos por terceros, incluidas las integrantes de un grupo financiero, las instituciones controladas

deberán observar lo siguiente: (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

20.1 Contar con políticas, procesos y procedimientos efectivos que aseguren una adecuada selección y calificación de los proveedores, tales como:

20.1.1 Evaluación de la experiencia pertinente;

20.1.2 Desempeño de los proveedores en relación con los competidores;

20.1.3 Evaluación financiera para asegurar la viabilidad del proveedor durante todo el período de suministro y cooperación previsto;

20.1.4 Respuesta del proveedor a consultas, solicitudes de presupuesto y de ofertas;

20.1.5 Capacidad del servicio, instalación y apoyo e historial del desempeño en base a los requisitos;

20.1.6 Capacidad logística del proveedor incluyendo las instalaciones y recursos; y,

20.1.7 La reputación comercial del proveedor en la sociedad.

20.2 Contratos debidamente suscritos y legalizados que contengan cláusulas que detallen, entre otros, los niveles mínimos de servicio acordado; las penalizaciones por incumplimiento; y, que prevean facilidades para la revisión y seguimiento del servicio prestado, ya sea, por la unidad de auditoría interna u otra área que la entidad designe, así como, por parte de los auditores externos o de la Superintendencia de Bancos y Seguros; y,

20.3 Contar con proveedores alternos que tengan la capacidad de prestar el servicio.

ARTÍCULO 21.- El manual que contempla el esquema de administración integral de riesgos, de que trata el artículo 15 del capítulo I "De la gestión integral y control de riesgos, incluirá la administración del riesgo operativo. (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

ARTÍCULO 22.- La Superintendencia de Bancos y Seguros podrá disponer la adopción de medidas adicionales a las previstas en el presente capítulo, con el propósito de atenuar la exposición al riesgo operativo que enfrenten las instituciones controladas. (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

Adicionalmente, la Superintendencia de Bancos y Seguros podrá requerir a las instituciones controladas, la información que considere necesaria para una adecuada supervisión del riesgo operativo.

ARTÍCULO 23.- En caso de incumplimiento de las disposiciones contenidas en este capítulo, la Superintendencia de Bancos y Seguros aplicará las sanciones correspondientes de conformidad con lo establecido en el capítulo I “Normas para la aplicación de sanciones pecuniarias”, del título XVI. (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

ARTICULO 24.- Los casos de duda y los no contemplados en el presente capítulo, serán resueltos por Junta Bancaria o el Superintendente de Bancos y Seguros, según el caso. (artículo renumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

SECCIÓN VII.- DISPOSICIONES TRANSITORIAS

PRIMERA.- Las instituciones controladas presentarán a la Superintendencia de Bancos y Seguros, hasta el 30 de abril del 2006, su diagnóstico y el proyecto de implementación de las disposiciones contenidas en este capítulo, para una administración adecuada del

riesgo operativo. El proyecto, debidamente aprobado por el directorio u organismo que haga sus veces, incluirá un cronograma detallado de las actividades que las instituciones controladas realizarán para su cumplimiento, señalando el responsable de cada una de ellas.

Para el caso de las cooperativas de ahorro y crédito que realizan intermediación financiera con el público, el plazo para la presentación del diagnóstico y proyecto de implementación será hasta el 31 de octubre del 2006.

SEGUNDA.- La implementación de las disposiciones previstas en este capítulo no podrá exceder de los siguientes plazos:

1.1 Para grupos financieros; y, para los bancos o sociedades financieras que no forman parte de un grupo financiero, las compañías de arrendamiento mercantil, las compañías emisoras y administradoras de tarjetas de crédito, las corporaciones de desarrollo de mercado secundario de hipotecas, las instituciones financieras públicas, hasta el 31 de agosto del 2009; y, (reformada con resolución No. JB-2008-1223 de 18 de diciembre del 2008)

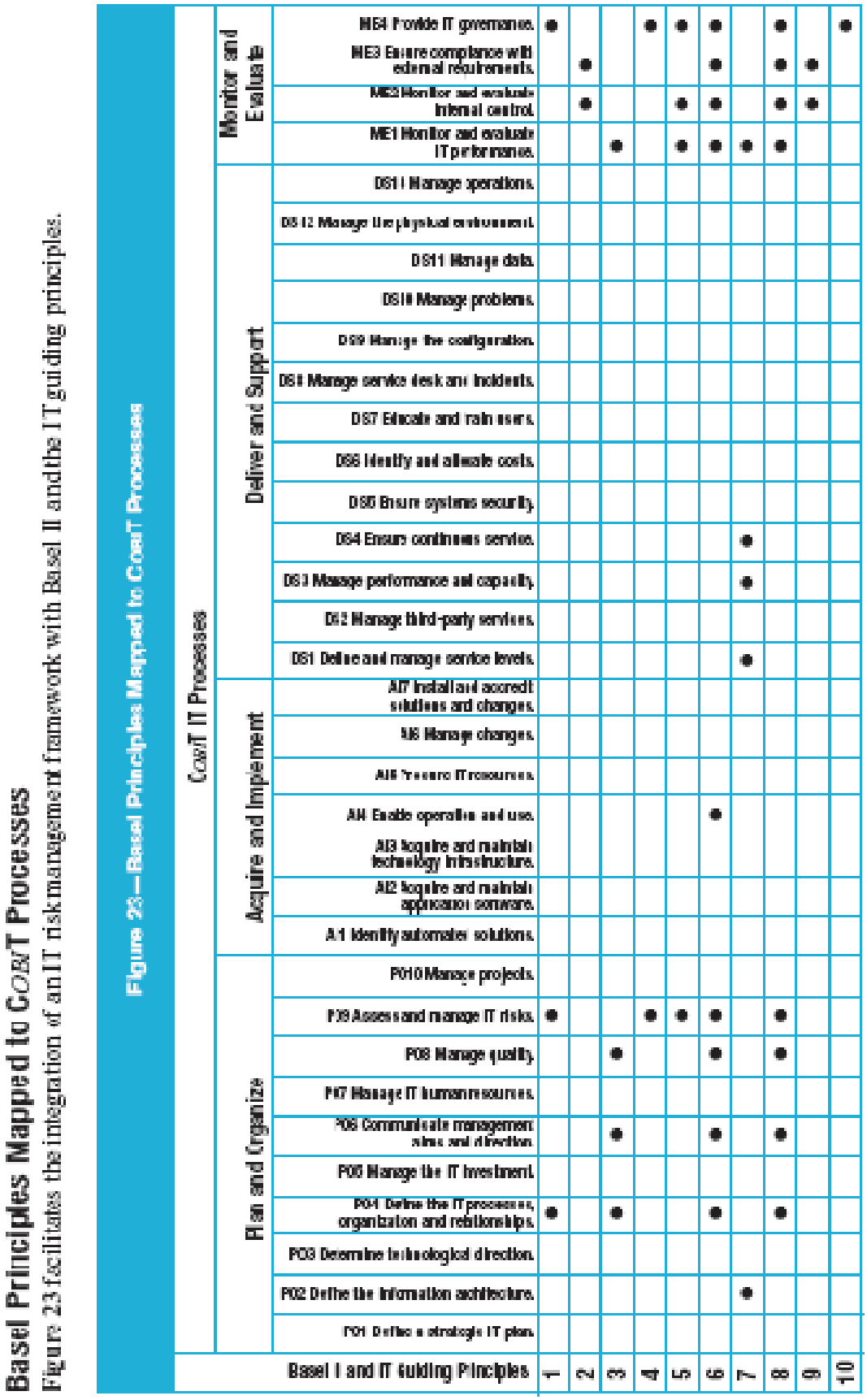
1.2 Para las cooperativas de ahorro y crédito que realizan intermediación con el público y las asociaciones mutualistas de ahorro y crédito para la vivienda, hasta el 31 de octubre del 2009. Esta fecha podrá ser modificada por el Superintendente de Bancos y Seguros, considerando el tamaño de la institución, la estructura organizacional, la cobertura geográfica y la complejidad de sus operaciones.

TERCERA.- El cumplimiento de las disposiciones constantes en el presente capítulo por parte de las instituciones del sistema financiero, deberá realizarse dentro de los plazos previstos en la disposición transitoria segunda, para cuyo efecto deberán ajustar sus planes de implementación de la norma de gestión de riesgo operativo, remitidos al organismo de control. (incluida con resolución No. JB-2008-1202 de 23 de octubre del 2008)

CUARTA.- Las instituciones del sistema financiero, hasta el 15 de enero del 2009, presentarán a este organismo de control un plan de acción que incluya las medidas que adoptarán para el cumplimiento de las disposiciones de este capítulo. El referido plan deberá ser aprobado por la Superintendencia de Bancos y Seguros. (incluida con resolución No. JB-2008-1223 de 18 de diciembre del 2008)

APÉNDICE 3. Principios de Basilea II mapeados con COBIT.

(Fuente: IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance. http://www.isaca.org)



Basel Principles Mapped to *CobiT* Processes

Figure 23 facilitates the integration of an IT risk management framework with Basel II and the IT guiding principles.

Bibliografía

[En línea] / aut. Asociación de Auditoría y Control de Sistemas de Información. - http://www.isaca.org/.
[En línea] / aut. Organización Internacional de Estándares. - http://www.iso.org/.
[En línea] / aut. Librería de Infraestructura de TI. - http://www.itil.co.uk/.
[En línea] / aut. Instituto de Ingeniería de Software. - http://www.sei.cmu.edu/cmmi.
[En línea] / aut. Ingeniería de Seguridad de Sistemas – Modelo de Madurez de Capacidades. - http://www.sse-cmm.org.
[En línea] / aut. Asociación de Contadores Públicos. - http://www.aicpa.org.
[En línea] / aut. Instituto Canadiense de Contadores Certificados. - http://www.cica.ca.
[En línea] / aut. Oficina de Contabilidad General de los Estados Unidos. - http://www.gao.gov.
[En línea] / aut. Information Technology Resources Board. - http://www.access-board.gov.
[En línea] / aut. Comité de Estándares del Instituto de Administración de Proyectos. - http://www.pmi.org.
Analisis de Cooperativas 2007 - 2008 [Informe] / aut. Superintendencia de Bancos y Seguros. - Quito : [s.n.], 2008.
Auditoría Informática: Un Enfoque Práctico [Libro] / aut. Piattini Mario. - [s.l.] : RA-MA, 2004.
Basel II: Aprovechamiento de las soluciones de gestión de los servicios empresariales para una excelente administración del riesgo [Informe] : Brouchure de producto / aut. BMC Software. - [s.l.] : BMC Software,Inc., 2006. - pág. 2. - http://www.bmc.com.
Boletín de Asesoría Gerencial [En línea] / aut. Epiñeira, Sheldon y Asociados // Riesgo Legal desde la perspectiva del Riesgo Operacional. - http://www.pwc.com/ve/spa/pdf/aseger_200808.pdf.
CAEFYC - Seminario Taller [Conferencia] / aut. MBA. Nelly Lucia Villacis, Master Ivonne Domínguez // Seguridad informática en el Marco de la Norma ISO 17799:2005. - Quito : [s.n.], ABRIL DEL 2007.
COBIT Mapping: Overview of International IT Guidance, 2nd Edition [Informe] / aut. Institute IT Governance. - 3701 Algonquin Road, Suite 1010 Rolling Meadows, IL 60008 USA : ITGI, 2006.
COBIT® Mapping: Mapping of ISO/IEC 17799: 2005 With COBIT® 4.0 [Informe] / aut. Institute IT Governance. - 3701 Algonquin Road, Suite 1010 Rolling Meadows, IL 60008 USA : ITGI, 2006.
COBIT® Mapping: Mapping of ITIL v3 With COBIT® 4.1 [Informe] / aut. Institute IT Governance. - 3701 Algonquin Road, Suite 1010 Rolling Meadows, IL 60008 USA : ITGI, 2008.
El Microcrédito en el Ecuador [Publicación periódica] / aut. Red Financiera Rural // Microfinanzas - Ecuador. - 2008.
Enciclopedia de la Seguridad Informática [Libro] / aut. Vieites Álvaro Gómez. - Madrid - españa : RA-MA, 2006.
Estadisticas del Sistema Financiero [En línea] / aut. Superintendencia de Bancos y Seguros. - Noviembre de 2008. - www.superban.gov.ec.
Evaluacion del Riesgo Operacional: Apropiado ambiente de gestion de elementos cualitativos [Conferencia] / aut. T. Jorge E. Olaya. - Guayaquil : Tecnologìa Avanzada del Ecuador, Septiembre, 2006.
Gobierno de las Tecnologías y los Sistemas de Información [Libro] / aut. V. Mario Piattini y Vidal Fernando Hervada. - Madrid : RA-MA, 2007. - pág. 456.
Identificación y Análisis de Riesgos [En línea] / aut. José Manuel Feria Domínguez. - http://thales.cica.es/rd/Recursos/rd98/Economia/02/texto3.html#R_reputacional.
IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance [Informe] / aut. IT Governance Institute. - 3701 Algonquin Road, Suite 1010 Rolling Meadows, IL 60008 USA : IT Governance Institute, 2007.
NETICOOP - UN ESPACIO COOPERATIVO EN LA RED [En línea] / aut. Giuseppina Da Ros - Red Universitaria de las Américas en Estudios Cooperativos y Asociativismo -UNIRCOOP- Universidad Asociada Pontificia Universidad Católica del Ecuador, Facultad de Economía, Quito - Ecuador Abril 2003. - http://www.neticoop.org.uy/rubrique10.html.
PROYECTO DE REGLAMENTO DE LA LEY DE COOPERATIVAS PARA LAS COOPERATIVAS DE AHORRO Y CREDITO [Informe].
Resoluciones de la Superintendencia de Bancos y Seguros [En línea] / aut. Superintendencia de Bancos y Seguros. - https://www.superban.gov.ec/downloads/normativa/2008/Junta_Bancaria/resol_JB-2008-1202.pdf.
Resumen de los Principios Clave de las Microfinanzas [Informe] : Resumen informativo / aut. CGAP. - Washington : [s.n.], 2004. - pág. 1. - http://cgap.org.

Seven Hurdles to IT & Physical Infrastructure Risk Management [Informe] / aut. Barnier Brian G.. - [s.l.] : ISACA E- Symposium - IBM Corporation, 27 January 2009.
Symantec [En línea] / aut. Symantec Corp. // Managing IT Risk. - 24 de Julio de 2007. - http://www.symantec.com/business/resources/articles/article.jsp?aid=managing_it_risk.