UNIVERSIDAD TECNICA DEL NORTE

INSTITUTO DE POSTGRADO

MAESTRIA EN CONTABILIDAD Y AUDITORIA

"Desarrollo de una Metodología de Evaluación al Sistema de Administración de Riesgo Operativo en la Cooperativa de Ahorro y Crédito Atuntaqui Ltda."

Requisito para la obtención del título de Magíster en Contabilidad y Auditoría

Autor: Ronald Fabián Macías Herrera

Tutor: Mgs. Marcelo Vallejos

Junio, 2017

APROBACIÓN TUTOR

En mi calidad de Tutor del presente proyecto presentado por el Ing. RONALD FABIAN MACIAS HERRERA, para optar por el título de MAGISTER EN CONTABILIDAD Y AUDITORÍA, cuyo tema es: **"Desarrollo de una Metodología de Evaluación al Sistema de Administración de Riesgo Operativo en la Cooperativa de Ahorro y Crédito Atuntaqui Ltda."** considero que el presente trabajo reúne requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del tribunal examinador que se designe.

En la ciudad de Ibarra a los 30 días del mes de mayo del 2017.

Mgs. Henry Marcelo Vallejos Orbe

C.C. 1001813821

TUTOR

APROBACIÓN JURADO EXAMINADOR

En calidad de jurado examinador del presente proyecto presentado por el Ing. RONALD FABIAN MACIAS HERRERA, para optar por el título de MAGISTER EN CONTABILIDAD Y AUDITORÍA, cuyo tema es: **"Desarrollo de una Metodología de Evaluación al Sistema de Administración de Riesgo Operativo en la Cooperativa de Ahorro y Crédito Atuntaqui Ltda.",** consideramos que el presente trabajo reúne requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del tribunal examinador que se designe.

En la ciudad de Ibarra a los 30 días del mes de mayo del 2017.

Mgs. Oswaldo Roberto Lara Castro

Mgs. Edison Benito Scacco Franco

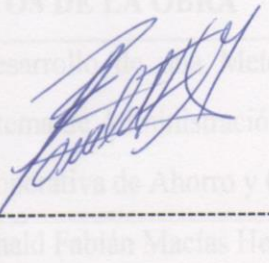
Mgs. Paúl Alexander Toro Echeverría

CESION DE DERECHOS

Yo, Macías Herrera Ronald Fabián, C.C. 100242025-3 manifiesto mi voluntad de ceder a la Universidad Técnica del Norte, los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor(es) del Trabajo de Tesis: **"Desarrollo de una Metodología de Evaluación al Sistema de Administración de Riesgo Operativo en la Cooperativa de Ahorro y Crédito Atuntaqui Ltda.",** que ha sido desarrollado para optar por el título de **MAGISTER EN CONTABILIDAD SUPERIOR Y AUDITORÍA,** en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En mi condición de autor(es) me reservo los derechos morales de la obra antes citada. En concordancia suscrita este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la biblioteca de la Universidad Técnica del Norte.

En la ciudad de Ibarra a los 30 días del mes de mayo del 2017.



RONALD MACIAS

CI: 100242025-3

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

La Universidad Técnica del Norte dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CEDULA DE IDENTIDAD	1002420253-3		
APELLIDOS Y NOMBRES	Macías Herrera Ronald Fabián		
DIRECCION	Barrio Los Ceibos		
EMAIL	rmacias@atuntaqui.fin.ec		
TELEFONO FIJO	062642341	**TELEFONO MÓVIL**	0982773984

DATOS DE LA OBRA	
TITULO	"Desarrollo de una Metodología de Evaluación al Sistema de Administración de Riesgo Operativo en la Cooperativa de Ahorro y Crédito Atuntaqui Ltda."
AUTOR (ES)	Ronald Fabián Macías Herrera
FECHA: AAAAMMDD	2017-05-30
PROGRAMA	Postgrado
TITULO POR EL QUE OPTA	Magister en Contabilidad y Auditoria
ASESOR/DIRECTOR	Magister Marcelo Vallejos

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Ronald Fabián Macías Herrera, con cédula de ciudadanía Nro.100242025-3, en calidad de autor (a) (es) y titular (es) de los derechos patrimoniales de la obra o trabajo de grado descrito

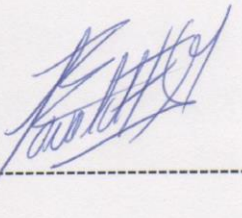
anteriormente, hago entrega del ejemplar respectivo en formato digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el repositorio digital institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la ley de Educación Superior Artículo 144.

3. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es la titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

En la ciudad de Ibarra a los 30 días del mes de mayo del 2017.

EL AUTOR



Ronald Fabián Macías

CI: 100242025-3

Facultado Por Resolución De Consejo Universitario ----------

DEDICATORIA

Dedico este trabajo a Dios, a mi esposa, a mis hijos y a mi familia que estuvieron junto a mí en el trayecto de este objetivo propuesto en mi vida,

Para toda mi familia por su apoyo, consejos, comprensión, amor, ayuda en todos los momentos difíciles para poder sacar lo mejor de mí como persona, como profesional y tener todo el coraje para poder conseguir este objetivo.

A mi esposa Adriana, agradecer por su paciencia y apoyo incondicional quien fue el pilar principal en la consecución de este objetivo.

"La dicha de la vida consiste en tener siempre algo que hacer, alguien a quien amar y alguna cosa que esperar". Thomas Chalmers

Ronald

AGRADECIMIENTO

En primer lugar quiero agradecer a Dios, por permitirme gozar de vida para poder llegar a este día y poder cumplir una meta más en mi existir. Lograr este objetivo no hubiera sido posible sin la ayuda de mi esposa, hijos, padres, hermanos, hijos y todos mis amigos que aportaron con su grano de arena en este proyecto.

A la UNIVERSIDAD TÉCNICA DEL NORTE por permitirme estudiar y ser una persona de bien y un gran profesional.

A mi director de tesis por el apoyo, esfuerzo y dedicación quien con sus conocimientos, su experiencia, experticia ha logrado que pueda cumplir con este documento.

También quiero agradecer a mis profesores de maestría que durante mi época de estudios lograron inculcarme conocimientos, motivación y principalmente por su amistad.

Si debería agradecer a todos esta página no me alcanzaría para nombrarlos, porque todas la personas que he conocido aportaron con algo muy representativo en el desarrollo de este proyecto, sin importar donde se encuentren, por su ayuda, inspiración, apoyo, buena vibra y por todas sus bendiciones muchas gracias que Dios les colme de bendiciones.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

DESARROLLO DE UNA METODOLOGÍA DE EVALUACIÓN AL SISTEMA DE ADMINISTRACIÓN DE RIESGO OPERATIVO EN LA COOPERATIVA DE AHORRO Y CRÉDITO ATUNTAQUI LTDA.

Autor: Ronald Fabián Macías Herrera

Tutor: Msc. Marcelo Vallejos

RESUMEN

El presente trabajo propone establecer una evaluación a la Administración de Riesgo Operativo de la Cooperativa de Ahorro y Crédito Atuntaqui; para ello se analizó la situación actual de la entidad, el desenvolvimiento de la misma en el mercado financiero, informes de Auditoría interna, informes de la Calificadora de Riesgos, y así poder definir el problema de investigación, fue necesario realizar un estudio de varios documentos, revistas, artículos, y parte fundamental una entrevista a un experto en riesgos, lo que permitió conocer a profundidad todo lo que abarca el Riesgo Operativo. Parte esencial de la investigación fueron los métodos, técnicas e instrumentos utilizados, identificando una secuencia eficaz para la obtención de la información respectiva, sin dejar a un lado el impacto que acarrea mencionado proyecto. Referente al análisis de los resultados se verificó su contraste con cada una de las preguntas de investigación y comprobar que el problema planteado es coherente, para posteriormente dar paso al establecimiento de la propuesta, en la cual se detalló de forma minuciosa las partes fundamentes de la metodología, pesos, ponderaciones, establecimiento de niveles, y consecutivamente se aplicó la metodología a la realidad de la Cooperativa, obteniendo una calificación cualitativa y cuantitativa respecto a la Administración de Riesgo Operativo, contrastando con cada una de las interrogantes de la investigación, con el objetivo general y verificando la solución al problema, y así poder establecer y conocer que estrategias son necesarias para que la entidad pueda mejorar e implementar nuevas políticas para el manejo del Riesgo Operativo.

DEVELOPMENT OF AN EVALUATION METHODOLOGY TO THE OPERATIONAL RISK ADMINISTRATION SYSTEM IN THE AUNRO CREDIT AND COOPERATIVE ATUNTAQUI LTDA.

Autor: Ronald Fabián Macías Herrera

Tutor: Msc. Marcelo Vallejos

SUMMARY

The present work proposes to establish an evaluation to the Operational Risk Administration of the Atuntaqui Savings and Credit Cooperative; To analyze the current situation of the entity, the development of the same in the financial market, Internal Audit reports, reports of the Risk Ratings, and thus to define the research problem, it was necessary to carry out a study of several documents , Magazines, articles, and an essential part of an interview with a risk expert, which allowed us to know in depth what is covered by Operational Risk. An essential part of the research was the methods, techniques and instruments used, identifying an efficient sequence for obtaining the respective information, without leaving aside the impact of the project. Regarding the analysis of the results, it was verified the contrast with each of the research questions and verified that the problem was coherent, to later give way to the establishment of the proposal, in which the detailed parts of the Methodology, weights, weights, establishment of levels, and consecutively applied the methodology to the reality of the Cooperative, obtaining a qualitative and quantitative qualification with respect to the Operational Risk Administration, contrasting with each one of the research questions, with the General objective and verifying the solution to the problem, so as to be able to establish and know what strategies are necessary for the entity to improve and implement new policies for the management of Operational Risk.

INTRODUCCIÓN

La Cooperativa de Ahorro y Crédito Atuntaqui Ltda., es una institución financiera ubicada en el segmento 1 al cual pertenecen las cooperativas más grandes del Sector de la Economía Popular y Solidaria, su principal fortaleza es el servicio de calidad y a tiempo que brinda a los socios.

En la actualidad las cooperativas de ahorro y crédito no han sido ajenas al impacto producido por la actual situación financiera del Ecuador, por tal motivo es indispensable para una institución financiera, contar con una adecuada gestión de riesgo que le permita evaluar oportunamente posibles eventos de riesgo y evitar pérdidas que afecten la situación financiera.

La gestión de riesgos conlleva a realizar acciones encaminadas a la identificación, medición, priorización, monitoreo, control y comunicación de las situaciones de riesgo, forjándose en todos los niveles organizativos de la empresa, evitando que existan errores en las estimaciones de los posibles impactos que deriven en consecuencias que no puedan ser subsanadas.

Los distintos tipos de riesgos de liquidez, mercado, crédito y operativo son de naturaleza distinta, notándose en la entidad objeto de la investigación un comienzo sostenido y anticipado en cuanto a su análisis; permitiendo a la entidad gestionar los riesgos relacionados con los cambios en el mercado, operaciones relacionadas con créditos concedidos y cumplimiento de las necesidades de efectivo de la entidad.

En cuanto al riesgo operativo, se trata del análisis y evaluación de errores humanos, tecnológicos, procesos y eventos externos que pueden poner en peligro a toda la entidad financiera e incluso llevarla a la quiebra, si no existen los controles para remediarlos.

La presente investigación tiene como objeto evaluar el sistema de Administración de Riesgo Operativo manejado en la COAC Atuntaqui, mencionado sistema engloba el desarrollo de las distintas etapas de identificación, medición, priorización, monitoreo, control y comunicación del riesgo operativo, aplicando procesos metodológicos de evaluación a la gestión del riesgo.

En el capítulo uno se revisarán algunos aspectos que permitan conocer a la Cooperativa de Ahorro y Crédito Atuntaqui Ltda, como antecedentes, el planteamiento y formulación del problema, sus justificaciones objetivos e interrogantes que surgen para el planteamiento del presente trabajo.

En el capítulo dos, se incluyen los aspectos conceptuales necesarios, normativa que rige actualmente el tema de estudio y que son indispensables para el desarrollo de los siguientes capítulos de la tesis operativa y por ende contar con las bases conceptuales para la propuesta que cumpla con el objetivo planteado.

Para el capítulo tres se analiza las distintas fases de la metodología que permitirán realizar una evaluación cuantitativa y cualitativa a la Administración de Riesgo Operativo, permitiendo tener claro el diseño metodológico aplicado en el desarrollo del presente trabajo.

En el capítulo cuatro se analizará lo referente al análisis e interpretación de los resultados, es decir en qué situación se encuentra la entidad, y que servirá como base para establecer la metodología a proponer para una eficaz Administración de Riesgo Operativo.

Seguidamente en el capítulo cinco, se detalla la metodología a proponer para la Evaluación del Riesgo Operativo, indicando de forma detallada los cálculos y procedimientos aplicados y que forman parte de la propuesta realizada en el proyecto de tesis establecido.

En el último capítulo se detallan las conclusiones y recomendaciones fruto del presente trabajo, en base a los resultados obtenidos a través de la aplicación de la metodología propuesta para evaluar y conocer el estado actual de la Administración de Riesgo Operativo en la COAC. Atuntaqui.

Anexo a los capítulos se adjunta las referencias bibliográficas, lincográficas utilizadas como fuente de información, que permitió sustentar y proponer todo lo detallado en los capítulos precedentes.

En definitiva, ésta tesis es un compendio que reúne la investigación de un tema de actualidad en el ámbito financiero local, nacional e internacional; que propone una gestión de riesgos anclada en una propuesta metodológica con un enfoque práctico y útil en la medición del nivel de gestión de Riesgo Operativo que mantienen las Cooperativas de Ahorro y Crédito del Sector Financiero Popular y Solidario; permitiendo un desenvolvimiento efectivo y el mejoramiento continuo de las mismas.

CAPÍTULO I

1. EL PROBLEMA

Este capítulo contiene los antecedentes, el planteamiento del problema, la formulación del problema, la justificación de la investigación, el objetivo general, objetivos específicos y las hipótesis o preguntas directrices que se persiguen para poder obtener los resultados planteados en la presente investigación.

1.1. Antecedentes

La Cooperativa de Ahorro y Crédito Atuntaqui nació en el cantón Antonio Ante, provincia de Imbabura, un día domingo 26 de mayo de 1963, el Padre Jorge Morales, párroco de Atuntaqui, anunció en la misa la visita del Sr. Carlos Flores, extensionista del Departamento de Educación de la Federación Nacional de Cooperativas de Ahorro y Crédito del Ecuador, quien sustentó una charla sobre cooperativismo en el salón de la Sociedad de Artesanos y esta invitación tuvo eco en un grupo de jóvenes amigos y noveleros que acudieron a la llamada, pero tan convincente debió haber sido la exposición que ese mismo día, entre broma y broma, constituyeron la Pre-cooperativa de Ahorro y Crédito "Atuntaqui" Ltda., recogiendo 200 sucres, de los cuales 65 correspondan a cuotas de ingreso y 135 por concepto de ahorros.

El primero de noviembre de 1963 fueron aprobados sus estatutos mediante Acuerdo No. 563; y su inscripción en el Registro General de Cooperativas se efectúo cinco días después. En diciembre de ese año el capital ahorrado ya sumaba 8.425 sucres y se concedieron los cuatro primeros préstamos de 2.100 sucres cada uno.

Desde su fundación hasta el año 1966 ocupó la presidencia el Sr. Juan Cadena Villegas y la función de Gerente General la asumió el Sr. Gonzalo Martínez Troya, quien con recibera en mano recorría las calles realizando las recaudaciones de los socios, sin recibir remuneración alguna por parte de la incipiente organización.

Hasta 1971 le sucedió en esa función el Sr. Saúl Vallejos Medina y luego el Sr. José Báez Villegas, quien permaneció en estas funciones hasta el año de 1996, para ser reemplazado por el Ingeniero Efrén Jácome y este por el Economista Ernesto Ortega. La Cooperativa de

Ahorro y Crédito “Atuntaqui” Ltda., entró al control de la Superintendencia de Bancos y Seguros a partir del año 1986.

1.2. Planteamiento del Problema

En el norte del país la intermediación financiera está soportada por un sinnúmero de entidades cuyo objetivo es el desarrollo socio económico de la región, brindando a la misma productos y servicios financieros que generen crecimiento y una rentabilidad sostenida.

De manera particular la Cooperativa de Ahorro y Crédito Atuntaqui Ltda. es una entidad dedicada a la intermediación financiera y se encuentra a la vanguardia del Sistema Cooperativo de todo el Ecuador demostrando honestidad, confianza, solvencia, seriedad y responsabilidad social al servicio de todos sus socios y clientes, factores que han permitido un desarrollo constante y han puesto en práctica el eslogan: “La Caja Fuerte del Ecuador”.

Se ha identificado que la entidad, cuenta con un Área de Administración de Riesgos, la cual cuenta con procedimientos definidos para la identificación, medición, priorización, control, mitigación y comunicación del riesgo de liquidez, mercado, crédito y operativo; este último denominado Riesgo Operativo y que es el objeto del presente proyecto de investigación. Para la Administración de Riesgo Operativo se cuenta con los procedimientos citados inicialmente, pero se carece de una evaluación realizada al sistema de gestión de riesgos, y que permita determinar el porcentaje de cumplimiento y efectividad del mismo referente al control del riesgo operativo; limitando la cuantificación de los avances e implementaciones que se realice por parte de la institución.

De igual manera no ha existido alguna autoevaluación a la gestión de Riesgo Operativo en la entidad, ni una Auditoría Especifica de riesgos que permita determinar fortalezas o debilidades que presente la actual Administración de Riesgos, siendo subjetivo el sustento que se pueda realizar respecto al estado actual y evolución que la entidad pueda haber atravesado en el transcurso de vida institucional.

En lo referente a la normativa anteriormente la COAC Atuntaqui estaba bajo el control de la SBS (Superintendencia de Bancos) quienes si manejan una normativa sobre Riesgo Operativo, pero actualmente la COAC está bajo la supervisión de la Superintendencia de Economía Popular y Solidaria, organismo de supervisión que no realiza un seguimiento o un control minucioso y progresivo a la gestión de riesgo Operativo. Un control administrativo que

permite garantizar que las actividades reales se ajusten a las actividades proyectadas permiten a cualquier entidad financiera desenvolverse en el mercado de intermediación financiera, el cumplimiento de las metas propuestas o proyectadas en un tiempo determinado.

"Ante circunstancias como las que viven el mundo de hoy, el comportamiento se modifica y nos enfrenta permanentemente a situaciones de ajuste, adaptación, transformación y desarrollo" (Aguilar, 2004, p.240), por tal motivo en toda organización se presentan eventos imprevistos que necesitan una respuesta inmediata y eficaz para mitigar el impacto negativo que pueda acarrear a la organización, pero si la entidad no evoluciona, o no conoce el estado actual de su gestión de riesgos, no estará en capacidad de medir y mejorar los procesos que requieran una atención específica. Procesos claros e identificados permiten a las entidades una versatilidad y adaptabilidad a un mercado de cambios constantes.

Finalmente, el no conocer de forma clara el nivel de gestión de riesgo operativo aplicado en la COAC Atuntaqui, limita fijar nuevas propuestas o establecer metodologías efectivas de medición a la gestión de Riesgos, elaboración de informes cuyas conclusiones o recomendaciones persigan la mejora continua de los procesos de control, limitando conocer la efectividad de actividades, procedimientos y procesos establecidos para la gestión de riesgo operativo, e impidiendo verificar la viabilidad de mitigación o reducción a los impactos generados por eventos de riesgo, por lo tanto es necesario y viable el establecimiento de una metodología que nos permita cuantificar el nivel de Administración de Riesgo Operativo aplicado en la COAC Atuntaqui.

1.3. Formulación del Problema

La cuantificación del nivel de Administración de Riesgo Operativo en la COAC Atuntaqui se fundamenta en un criterio personal, sin establecer una metodología que sustente el nivel de riesgo operativo obtenido para un evento suscitado.

1.4. Justificación de la Investigación

La realización del presente estudio de investigación se fundamenta en poder identificar el estado actual de la Administración Integral de Riesgo Operativo, e identificar la evolución de mencionada administración en beneficio de la Cooperativa Atuntaqui. Tomando la definición de riesgo operativo y haciendo hincapié en los factores que lo conforman, como las personas, recurso principal de cualquier organización, siendo un recurso primordial para el

desempeño o consecución de cualquier objetivo, es necesario que el recurso humano tenga un control adecuado, se debe tomar en cuenta que las personas son las encargadas de manejar o administrar todo tipo de sistemas, y para el correcto desempeño de las mismas, los procesos en los cuales están inmiscuidos deben estar establecidos de manera correcta. Procesos bien implementados permiten que las actividades y procedimientos realizados por las personas fluyan de la mejor manera y permita la consecución de las metas propuestas.

Otro factor primordial y propio de la época, es la tecnología de la información, la cual es responsable de la evolución en todos los campos del mercado financiero, las entidades que no han realizado inversión alguna en tecnología de la información han desaparecido o han sido absorbidas por la empresas o compañías que sí lo han hecho. Pero así como la tecnología de información evoluciona con el fin de mejorar los controles de protección a la información de las entidades, también evolucionan los medios cuyo objetivo es el daño o hurto de información confidencial, por lo tanto la mejora continua ,actualizaciones, debe ser constantes y periódicas para poder mitigar y controlar todos los riesgos que puedan presentarse en las operaciones diarias de una entidad y al mismo tiempo estar a la vanguardia de los mejoramientos presentados diariamente en el campo tecnológico.

Finalmente y no menos importantes el último factor son los eventos externos, que se refieren a daños físicos que pueden ser ocasionados por circunstancias naturales o humanas ajenas a la voluntad de la entidad, por lo tanto no se puede prevenir su ocurrencia, pero si se puede estar preparados para poder disminuir los impactos generados a través de planes contingentes que permitan mantener la continuidad del negocio, un mínimo tiempo de recuperación de actividades.

Por lo tanto al no conocer de forma claro el estado actual de la Administración de Riesgo Operativo de la entidad, es imposible proponer mejoras o implementaciones con las cuales se pueda identificar los resultados alcanzados y beneficios obtenidos por la implementación de nuevas estrategias de riesgos.

1.5. Objetivos

1.5.1. General

Cuantificar el nivel de Administración de Riesgo Operativo en la Cooperativa de Ahorro y Crédito Atuntaqui Ltda.

1.5.2. Específicos

- Diagnosticar la situación actual de la Administración de Riesgo Operativo en la Cooperativa de Ahorro y Crédito Atuntaqui Ltda.
- Analizar la aplicación de las Normas Generales para las Instituciones del Sistema Financiero referentes a la gestión del Riesgo Operativo.
- Desarrollar la Metodología de cálculo para medir los niveles de Gestión de Riesgo Operativo.

La consecución de estos objetivitos se cumplirá respondiendo las siguientes interrogantes:

1.5.3. Interrogantes de la Investigación

1. ¿Cuál es la situación actual de la Administración de Riesgos en la Cooperativa de Ahorro y Crédito Atuntaqui Ltda.?
2. ¿Cómo se realiza actualmente la aplicación de las normas generales para las instituciones del Sistema Financiero referente a la Gestión de Riesgo Operativo?
3. ¿Cuál es el nivel de Administración de Riesgo Operativo en la Cooperativa de Ahorro y Crédito Atuntaqui Ltda.

CAPÍTULO II

2. MARCO REFERENCIAL

El presente capítulo trae consigo la definición de cada uno de los temas que forman parte en el presente trabajo de investigación, mediante la citación de definiciones realizadas por autores con publicaciones actualizadas y reconocidas, normativas y disposiciones nacionales e internacionales con el objetivo de poder determinar definiciones propias y que permitan el cumplimiento de los objetivos propuestos.

2.1. Diagnóstico Organizacional

Para poder cumplir el primer objetivo se debe tener claro a lo que se refiere el diagnóstico a realizar en la institución, por lo tanto se procede a citar la siguiente definición:

Arizabaleta (2004) afirma:

> *En términos muy sencillos definiremos el diagnóstico como un proceso de comparación entre dos situaciones: la presente, que hemos llegado a conocer mediante la indagación, y otra ya definida y supuestamente conocida que nos sirve de pauta o modelo. El "saldo" de esta comparación o contraste, es lo que llamamos diagnóstico. (p.20).*

Scarón de Quintero (1985) afirma:

> *El diagnóstico es un juicio comparativo de una situación dada con otra situación dada" ya que lo que se busca es llegar a la definición de una situación actual que se quiere transformar lo que se compara, valorativamente con otra situación que sirve de norma o pauta. (p. 26).*

Respecto al diagnóstico Organizacional Prieto Herrera (2009) menciona que es *"un proceso que permite establecer los puntos fuertes y débiles, las fuerzas restrictivas, la dinámica del cambio, el sistema operacional y la salud de una organización"* (p.22).

Con estas tres definiciones es fácil llegar a establecer que el diagnóstico organizacional obedece al establecimiento de las fortalezas y debilidades de una organización; conocer los puntos fuertes, débiles, en otras palabras conocer la situación actual de la institución y su capacidad de respuesta ante eventos que puedan presentarse, con un solo propósito que es la mejora continua.

2.2. Estructura organizacional

Para el análisis de la Estructura Organizacional, se ha tomado la definición de los siguientes autores, según se detalla a continuación:

Para Soto Concha (2009) la estructura organizacional es el *"marco formal mediante el cual las tareas se dividen agrupan y coordinan"* (p.8).

Otra definición detalla que *"la estructura organizacional comprende la forma en que la organización divide el trabajo y realiza su posterior coordinación, buscando la concordancia entre los procesos internos y el entorno (Head, 2005; Lee y Grover, 1999; Lenz, 1980)"* (Marín Idárraga & Losada Campos, Estructura organizacional y relaciones inter-organizacionales: análisis, 2015).

Para finalizar Marín Idárraga (2012) afirma:

> *Así, la estructuración de las organizaciones puede asumirse como un patrón de variables creadas para coordinar el trabajo de los agentes organizacionales, resultante de los procesos de división del mismo, que generan rutinas formalizadas, diferenciadas y estandarizadas, intentando controlar y hasta predecir su comportamiento (Ackoff, 2000; Daft & Steers, 1992; Galbraith, 2001; Litterer, 1979; Mintzberg, 1984; Nadler & Tushman, 1997).*

Por tal motivo la estructura organizacional se enfoca a la forma en que se divide y organiza el trabajo en una organización, identificando la estructura funcional de la institución, los procesos gobernantes, productivos y de apoyo con el objetivo de conocer de manera clara las áreas y sus funciones asignadas acorde a los objetivos de la institución.

2.3. Administración Integral de Riesgos

Para partir con el análisis de la Administración Integral de riesgos, la principal fuente son las Normas Generales para las instituciones del Sistema Financiero, en el Titulo X.- De la Gestión y Administración de Riesgos, en EL Capítulo I, Artículo 2, numeral 2.2 define a la Administración de Riesgos como:

> *El proceso mediante el cual las instituciones del sistema financiero identifican, miden, controlan / mitigan y monitorean los riesgos inherentes al negocio, con el objeto de definir el perfil de riesgo, el grado de exposición que la institución está dispuesta a asumir en el desarrollo del*

> *negocio y los mecanismos de cobertura, para proteger los recursos propios y de terceros que se encuentran bajo su control y administración.*

Por otra parte Casares (2013) afirma:

> *La administración de riesgos es el proceso administrativo formal para identificar, medir, controlar y supervisar los distintos riesgos a los que están expuestas las empresas, para que con base en esta información se pueda realizar una adecuada gestión de los riesgos y establecer el efecto de las contingencias detectadas en el nivel de solvencia de la empresa. (p.26).*

Por lo tanto la administración de Riesgos es un proceso que se fundamenta en identificar, medir, priorizar, controlar, mitigar, monitorear y comunicar los riesgos que pueden afectar a la organización y así definir el perfil de riesgos de procesos, procedimientos o eventos que se pueden presentar de forma periódica y paralelamente definir las acciones a realizar para identificar el impacto que afrontará la entidad.

2.4. Riesgo

Las Normas Generales para las instituciones del Sistema Financiero, en el Titulo X.- De la Gestión y Administración de Riesgos, en EL Capítulo I, Artículo 2, numeral 2.1 definen al riesgo como “la posibilidad de que se produzca un hecho generador de pérdidas que afecten el valor económico de las instituciones”.

Pérez Barbeito (2014) afirma:

> *El riesgo se asocia con lo inesperado, con lo no deseado. Una definición más aceptable señala que el riesgo es cualquier variación en un resultado respecto al esperado. Esta definición es útil porque incluye tanto los resultados deseables como los no deseables. (p. 199).*

López Parra (2004) menciona:

> *Por riesgo entendemos la probabilidad de que la empresa no pueda enfrentar alguna situación inherente a su actividad. Esta definición es muy general pero, como veremos más adelante, son por lo menos tres riesgos los que nos permiten evaluar la situación, los resultados y el entorno de la empresa. (p.70).*

Castillo & Mendoza (2002) citan el siguiente texto:

(Jorion, 2000) define el riesgo como «la volatilidad de los resultados esperados, generalmente el valor de activos o pasivos de interés». *De acuerdo con el tipo de factores o variables que lo generen, el riesgo en las corporaciones se suele agrupar en cuatro grandes categorías: Riesgo de Mercado, Riesgo de Crédito, Riesgo Estratégico o de Negocio y Riesgo Operacional.* (p.46).

Tomando el criterio de los autores mencionados anteriormente y lo expuesto en la normativa, el riesgo está asociado ampliamente a la estadística, porque es la posibilidad de que pueda o no producirse un hecho o un acto que genere un impacto económico a la organización y por ende afecte al valor económico de la empresa.

2.5. Riesgo Operativo

Adentrados en la Administración de Riesgos, se puede identificar el campo al cual se desea analizar, para el caso de este estudio, el análisis se enfoca al Riesgo Operativo, el cual según Las Normas Generales para las instituciones del Sistema Financiero, en el Titulo X.- De la Gestión y Administración de Riesgos, en el Capítulo I, Artículo 2, numeral 2.9 lo define como:

> *La posibilidad de que se produzcan pérdidas debido a eventos originados en fallas o insuficiencia de procesos, personas, sistemas internos, tecnología, y en la presencia de eventos externos imprevistos. Incluye el riesgo legal pero excluye los riesgos sistémico y de reputación. Agrupa una variedad de riesgos relacionados con deficiencias de control interno; sistemas, procesos y procedimientos inadecuados; errores humanos y fraudes; fallas en los sistemas informáticos; ocurrencia de eventos externos o internos adversos, es decir, aquellos que afectan la capacidad de la institución para responder por sus compromisos de manera oportuna, o comprometen sus intereses.*

En un artículo publicado por Castillo & Mendoza (2002) menciona: *"El Comité de Basilea ha definido el riesgo operativo como «el riesgo de pérdida causada por falla o insuficiencia de procesos, personas y sistemas internos, o por eventos externos» (Bassel Committee on Banking Supervision, 2003)"* (p.46).

Adentrandóse al tema de estudio, el Riesgo Operativo se basa en cuatro factores: las personas, procesos, tecnología de la información y eventos externos, los cuales son factores

que están presentes en todas las áreas de la organización y que su control conlleva a mitigar cualquier impacto negativo que logre sobrepasar las barreras de los controles implementados.

2.5.1. Factores de Riesgo Operativo

Al adentrarse al análisis del Riesgo Operativo, se debe considerar las fuentes o factores de riesgo operativo, las cuales se agrupan en 4 grandes categorías: Personas, procesos, tecnología de la información y eventos externos.

Respecto al análisis de las personas Palma Rodríguez (2011) afirma: ***"****Este riesgo está relacionado con la posibilidad de pérdidas financieras asociadas con negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, lavado de dinero, inapropiadas relaciones interpersonales y ambiente laboral desfavorable"* (p.631).

Las Normas Generales para las instituciones del Sistema Financiero, en el Titulo X.- De la Gestión y Administración de Riesgos, en el Capítulo V, Artículo 4, numeral 4.2 mencionan lo siguiente sobre el factor 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. (p.631).*

Respecto al factor procesos se cuenta con las siguientes definiciones:

Palma Rodríguez (2011) afirma: *"Procesos Internos: Identifica la posibilidad de incurrir en pérdidas debido a fallas en los procesos, políticas o procedimientos inadecuados o inexistentes que pueden ocasionar la suspensión de servicios o bien el desarrollo deficiente de operaciones"* (p.631).

Las Normas Generales para las instituciones del Sistema Financiero, en el Titulo X.- De la Gestión y Administración de Riesgos, en el Capítulo V, Artículo 4, numeral 4.2 mencionan lo siguiente sobre el factor 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" (p.630).

Como tercer factor y no menos importante se debe analizar la Tecnología de Información, Palma Rodríguez (2011) indica que *"los fallos tecnológicos pueden ocasionar pérdidas financieras derivadas del uso inadecuado de sistemas de información y tecnologías relacionadas, que pueden afectar el desarrollo de las operaciones y servicios"* (p.631).

Las Normas Generales para las instituciones del Sistema Financiero, en el Titulo X.- De la Gestión y Administración de Riesgos, en el Capítulo V, Artículo 4, numeral 4.2 mencionan lo siguiente sobre el factor tecnología de la información indica:

> *Las instituciones controladas deben contar con la Tecnología de la 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. (p.632).*

Un factor trascendental en el análisis de Riesgo Operativo son los eventos externos, Palma Rodríguez define (2011):

> *Este grupo comprende la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos al control de la empresa que pueden alterar el desarrollo de sus actividades, afectando a los procesos internos, personas y tecnología de información. Por ejemplo las fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, así como las fallas en servicios críticos provistos por terceros. Otros riesgos asociados con eventos externos incluyen: el rápido paso de cambio en las leyes, regulaciones o guías, así como el riesgo político o del país. (p.631).*

Las Normas Generales para las instituciones del Sistema Financiero, en el Titulo X.- De la Gestión y Administración de Riesgos, en el Capítulo V, Artículo 4, numeral 4.2 mencionan lo siguiente sobre el factor eventos externos indican:

> *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. (p.644).*

De forma resumida los factores como las personas, procesos, tecnología de la información y eventos externos son pilares que deben poseer controles minuciosos por parte de la Administración de Riesgos, con procedimientos adecuados de identificación, de medición, control, priorización, mitigación y comunicación, y dentro de cada uno de estos procedimientos cuando amerite es indispensable contar con planes de contingencia y continuidad con el único objetivo de mantener las continuidad de las actividades.

Dentro del analisis de Riesgo Operativo la Seguridad de la Informacion es un punto clave para obterner resultados eficaces, ciertos autores la mencionan como parte de la criptología, para obtener una idea mas clara, Molina Mateos (2000) define a la criptología como "la ciencia que estudia los principios, medios, métodos, sistemas, procedimientos y algoritmos de cifrado y descifrado de la información y las comunicaciones, su clasificación en función de los riesgos, análisis y evaluación".

Y respecto a la seguridad de la informacion el mismo Molina Mateos (2000) afirma:

> *La seguridad de la información viene determinada por los peligros, riesgos y amenazas a que puede verse sometida la información. La variedad e intensidad de los riesgos y amenazas son tan diversas que, a "priori", resulta extremadamente difícil establecer "la seguridad necesaria". Si además se tiene en cuenta la diferencia entre la lógica del razonamiento del atacante, que en definitiva es el que puede elevar el nivel de exigencia de seguridad, y la lógica de razonamiento del que elabora la defensa, que para ser efectiva la seguridad ha de ser superior a los niveles de agresiones potenciales. Por todo ello, resulta evidente la dificultad y complejidad del diseño de criterios de seguridad.*

Areitio Bertolín (2008) afirma:

> *La seguridad de la información es un proceso en el que se da cabida a un creciente numero de elementos: aspectos tecnologicos, de gestión-organizacionales, de recursos humanos, de índole economica, de negocios, de tipo legal, de cumplimiento, etc.; abarcando no sólo aspectos informáticos y de telecomunicaciones sino tambien aspectos fisicos, medioambientales, humanos, etc.*

Para Costas Santos (2014), la seguridad de la informacion consiste:

> *En asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información*

allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

La seguridad de la informacion tiene como objetivo el control de los riesgos que puedan originarse y a su vez afectar a la informaciòn de la entidad, con el unico objetivo de establecer las seguridades necesarias, mediante la implementaciòn de insumos tecnològicos, mejora en los procesos, actualizacion de aspectos tecnològicos y telecomunicaciones para que los usuarios tengan la plena confianza de usar los canales electrònicos institucionales.

2.6. Continuidad del Negocio

Dentro de la administración eficiente del Riesgo Operativo la continuidad del Negocio es parte fundamente en la operatividad de las actividades institucionales:

Las Normas Generales para las instituciones del Sistema Financiero, en el Titulo X.- De la Gestión y Administración de Riesgos, en el Capítulo V, Artículo 15 mencionan lo siguiente sobre la continuidad del Negocio: ***"****Las instituciones controladas deben administrar la continuidad del negocio, manteniendo procedimientos actualizados, a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción del negocio"* (p.647).

Por su parte Martínez (2004), menciona que: "si estos procedimientos se refieren a la restauración de las funciones críticas de la organización, con independencia del Departamento en que dichas funciones sean realizadas, estamos hablando de operaciones de recuperación de la continuidad del negocio".

La continuidad del negocio se refiere a que las operatividad de la institución no debe detenerse por nada, si se cuenta con un canal o medio principal, siempre debe existir un medio alterno, que en otras palabras es la contingencia al control; se deja claro que no se puede eliminar los impactos que puedan producir algún evento de riesgo, pero si se puede mitigarlo, trasladarlo, y que el riesgo residual a asumir pueda ser soportado por la entidad sin problema alguno.

2.7. Normas Generales y Resoluciones entes de control

La Cooperativa Atuntaqui anteriormente estaba bajo la supervisión de la Superintendencia de Bancos, quien emitió en el año 2004 normas generales para la

administración del Riesgo Operativo, posteriormente con el paso al control de la Superintendencia de Economía Popular y Solidaria, se mantuvo vigente el cumplimiento de la normativa emitida en el año 2004, y se añadió resoluciones de control y cumplimiento mínimo en la Administración de Riesgos.

2.7.1. Resolución No. 128-2015-F

Una parte fundamental que deben tomar en cuenta las instituciones del sistema financiero son las normas, resoluciones emitidas por los entes de control, en su tiempo la Superintendencia de Bancos y Seguros y actualmente la Superintendencia de Economía Popular Solidaria. En el año 2015. La Junta de Regulación Monetaria y Financiera emitió una resolución el 23 de septiembre del 2015, mencionada Resolución mantiene las normas para la Administración de Riesgos en las Cooperativas de Ahorro y Cajas Centrales, mencionada ley es parte fundamental para poder comenzar con una buena Administración de Riesgo Operativo.

2.7.2. Libro I.- Normas Generales para las Instituciones del Sistema Financiero TITULO X.- De la Gestión y Administración de Riesgos, CAPÍTULO V.- De la Gestión del Riesgo Operativo; mencionada norma esta en base a la resolución No JB-2005-834 de 20 de octubre del 2005.

Mencionada Norma contiene varias Secciones, el artículo 1 que es una introducción a la misma, definiciones, factores de Riesgo Operativo, la administración de Riesgo Operativo, Continuidad del Negocio, responsabilidades en la Administración de Riesgo Operativo, Servicios Provistos por Terceros, Seguridad de la Información.

2.7.3. Normas ISO 31000

La norma ISO 31000 trata sobre la Gestión de Riesgos – Principios y Guías, en la presente norma se realiza una breve introducción sobre la gestión de riesgos, indicando los beneficios que trae consigo una correcta gestión, posteriormente se detalla el ámbito de aplicación, definiciones, marco de gestión de riesgos, estructura de la guía de trabajo. Finaliza con establecer la definición de Riesgos, la evaluación de Riesgos, tratamiento de los riesgos, y concluye con los atributos de la mejor gestión del riesgo.

2.8. Metodología de Cálculo

Para establecer el concepto de metodología se ha tomado el siguiente criterio de Báez Paz (2014) quien menciona que *"la metodología ejerce el papel de ordenar, se apoya en los métodos, como sus caminos y éstos en las técnicas como los pasos para transitar por esos caminos del pensamiento a la realidad y viceversa"* (p.43).

De igual manera Báez Paz (2014) indica que

> *El método constituye a la vez un orden y un proceso cuya culminación es la construcción de leyes, teorías y modelos. Por esta razón, las leyes, las teorías y los modelos son, para el científico, la medida del éxito o del fracaso de una investigación. (p.43).*

Navarro Chávez (2014) expone lo siguiente:

> *Etimológicamente metodología significa tratado del método, método significa ir a lo largo (buen) camino, es decir, forma de proceder en cualquier dominio y de ordenar la actividad a un fin (Bochenski, 1971, 32) y Mario Bunge (2006) hace una advertencia: La metodología es el estudio de métodos, la investigación sustancial utiliza métodos, no metodologías" (p.17-18).*

Al establecer la metodología para el presente proyecto de tesis, es ordenar cada requerimiento de la normativa respecto a la gestión de Riesgo Operativo, con el objetivo de poder medir y evaluar el grado de efectividad de los procesos o procedimientos aplicados para la actual administración, en este caso del riesgo operacional.

2.9. Niveles de Gestión de Riesgos

Rubio Romero (2002) acota:

> *El término gestión, tan utilizado en la actualidad, puede definirse como hacer diligencias para conseguir una cosa. Según Manuel López Cachero (1998:10) se define como la «ordenación metódica de actividades interdependientes y procedimientos relacionados que posibilita el buen hacer de una organización», mientras que la norma UNE-EN ISO 9000:2000, lo define como las «actividades coordinadas para dirigir y controlar una organización». Por lo tanto, si la empresa voluntariamente se plantea el objetivo de eliminar o al menos reducir y controlar sus riesgos y reducir los costes de los incidentes, accidentes y enfermedades profesionales, va a necesitar desde el punto de vista técnico, gestionar las actividades dirigidas en este sentido.*

Mejía Delgado (2011) define a la gestión como *"el proceso de planear, dirigir, organizar y controlar los recursos y actividades de una empresa, para reducir al mínimo, el efecto económico al ocurrir un riesgo, al menor costo posible".*

Respecto a la definición de niveles, Mejía Hernán (2011) afirma:

El grado de peligrosidad de las amenazas que gravitan sobre una empresa se puede expresar en forma matemática, como una medida de los riesgos que presenta cada uno, a fin de aplicar medidas para evitar su ocurrencia o reducir sus efectos.

Por lo tanto los niveles de gestión de Riesgos se refiere al proceso de planear, dirigir, organizar y controlar los recursos de la entidad a través de establecimiento de grados de peligrosidad o riegos producidos por las amenazas y a través de una medida o calificación establecer el grado de efectividad en la Administración, en el caso del presente estudio enfocado al Riesgo Operativo.

CAPÍTULO III

3 MARCO METODOLÓGICO

En el presente capítulo se analizará las distintas fases de las metodologías utilizadas para realizar la evaluación al Sistema de Administración de Riesgo Operativo de la Cooperativa Atuntaqui, mediante la aplicación de métodos de investigación.

3.1. Descripción del área de estudio

El área de estudio de la presente investigación es el área de Riesgos de la COAC Atuntaqui, la cual es la encargada de la identificación, medición, control, mitigación y comunicaciones de los eventos de Riesgo Operativo que puedan presentarse. Como se indicaba en la parte teórica, los factores que inciden el Riesgo Operativo son las personas, procesos, tecnología de la información y eventos externos, los cuales se direccionan a toda la entidad.

Por lo tanto la aplicación de todos los procedimientos adecuados, cumplimiento de normativa forman parte de un sistema de Administración de Riesgo Operativo, el cual para un pleno cumplimiento de la normativa y disposiciones legales debe presentar documentos, metodologías, manuales, procesos, políticas, etc. La idea de este proyecto es poder establecer desde el interior del área de Riesgos, una autoevaluación de los procesos y procedimientos realizados actualmente, que permitan mitigar al máximo los impactos de los posible los eventos de Riesgo, manteniendo vigente la mejora continua de los mismos.

3.2. Tipo de Investigación

Para el análisis del presente trabajo los tipos de investigación a aplicar son la investigación cuantitativa, cualitativa, documental y descriptiva.

Para la consecución de los objetivos identificados en el presente proyecto se plantea realizar una investigación de carácter cualitativo y cuantitativo, sintetizándose en una investigación mixta. Hay que tener claro según Hernández Sampieri, Fernández Collado, & Baptista Lucio (2010) respecto a la meta de la investigación mixta *"no es reemplazar a la investigación cuantitativa ni a la investigación cualitativa, sino utilizar las fortalezas de ambos*

tipos de indagación combinándolas y tratando de minimizar sus debilidades potenciales". (p. 544)

En el caso de la presente investigación es necesario analizar desde un punto de vista cualitativo las circunstancias que han motivado a la entidad al cumplimiento o no de las resoluciones del ente de control, y mediante el análisis matemático o de valores establecer valores o medidas que permitan determinar el nivel de administración de Riesgo Operativo.

Para determinar que la investigación es de carácter cualitativa, se toma como referencia la siguiente acotación según Tamayo (2003) quien manifiesta lo siguiente:

> *La investigacion cualitativa es humanista, el investigador cualitativo busca acceder por distintos medios a lo personal y a la experiencia particular del modo en que la misma se percibe, se siente, se piensa y se actúa por parte de quien la genera o la vive. (p.60)*

El termino cualitativo se refiere especificamente a las cualidaddes que le caractiza al objeto de investigación, es más de carácter humano y social. En el caso del Riesgo Operativo dentro de los factores de estudio se analiza a las personas, y los impactos que un error humano puede ocasionar de forma economica a la entidad.

Exáctamente lo que busca esta investigación es conocer ciertos temas relacionados a las personas o colaboradores de la Cooperativa Atuntaqui, y poder identificar a traves de un análisis la aplicación o no de la normativa, los motivos por los cuales se tomó la decisión de aplicar o no y las incidencias que esto representa para la entidad.

Respecto a la investigación cuantitativa, para poder analizar y evaluar a la administración de Riesgo Operativo, analizarlo desde un punto de vista cuantitativo, permite conocer de forma más acertada una correcta Administración de Riesgo Operativo. Bernal (2010) asevera:

> *El método cuantitativo o método tradicional se fundamenta en la medición de las características de los fenómenos sociales, lo cual supone derivar de un marco conceptual pertinente al problema analizado, una serie de postulados que expresen relaciones entre las variables estudiadas de forma deductiva, este método tiende a generalizar y normalizar resultados (p. 60).*

A esta definición Hernández Sampieri, Fernández Collado, & Baptista (2010) argumentan que enfoque cuantitativo (que representa, como dijimos, un conjunto de procesos)

es secuencial y probatorio y que cada etapa precede a la siguiente y no podemos brincar o eludir, el orden es riguroso, aunque, desde luego, podemos redefinir alguna fase. *Parte de una idea, que va acotándose y, una vez delimitada, se derivan objetivos y preguntas de investigación, se revisa la literatura y se construye un marco o una perspectiva teórica….(p. 4).*

En la parte superior se hace referencia a la investigación de carácter descriptivo y documental; según Bernal (2010) afirma: *"La investigación documental consiste en un análisis de la información escrita sobre un determinado tema, con el propósito de establecer relaciones, diferencias, etapas, posturas o estado actual del conocimiento respecto al tema objeto de estudio"* (p. 112) y respecto a la investigación descriptiva el mismo Bernal (2010) acota: *"Investigación descriptiva busca especificar propiedades, características y rasgos importantes de cualquier fenómeno que se analice. Describe tendencias de un grupo o población*" (p. 80) Apoyado en estas deficiones se puede argumentar que dentro de los antecedentes se analiza la normativa institucional, Manual Integral de Riesgos que contiene políticas, procedimientos, metodologías, para poder establecer si requiere actualización alguna mencionada normativa institucional y compararla con las normas emitidas por los organismos de control.

En el diagnóstico situacional de la Administración de Riesgo Operativo, se ha utilizado el método descriptivo y documental, a través de técnicas de investigación que dependen de una correcta *"recolección de datos que según Tamayo (2003) sostiene que depende en gran parte del tipo de investigación y del problema planteado para la misma, y puede efectuarse desde la simple ficha bibliográfica, observación, entrevista, cuestionarios o encuestas y aun mediante ejecución de investigaciones para este fin*…(p. 182), por lo tanto a través de la una entrevista con personas expertas en Riesgos, se puede establecer la metodología más óptima de evaluación a la Administración de Riesgos de la COAC. Atuntaqui.

3.3 Métodos de Investigación

Para la consecución de los objetivos identificados en el presente trabajo, los métodos que se aplique en la investigación son fundamentales, por lo tanto referente a los métodos a utilizar, enfocado en el método deductivo Bernal (2003) menciona:

> *Este método de razonamiento consiste en tomar conclusiones generales para obtener explicaciones particulares. El método se inicia con el análisis de los postulados, teoremas, leyes,*

> *principios, etcétera, de aplicación universal y de comprobada validez, para aplicarlos a soluciones o hechos particulares. (p.59).*

Es lo que busca el presente trabajo de investigación, tomar conclusiones generales, para poder transformarlas en conclusiones a la medida de la Cooperativa Atuntaqui, estableciendo metodologías de evaluación que permitan conocer de forma más clara la situación institucional en base al riesgo.

De igual manera en el desarrollo de ciertos temas en el presente proyecto, existen eventos de Riesgo muy particulares de la institución, pero que sí pueden ser considerados como base en el análisis a otras entidades financieras, por lo tanto referente al método inductivo Bernal (2003) menciona:

> *Este método utiliza el razonamiento para obtener conclusiones que parten de hechos particulares aceptados como válidos, para llegar a conclusiones cuya aplicación sea de carácter general. El método se inicia con un estudio individual de los hechos y se formulan conclusiones universales que se postulan como leyes, principios o fundamentos de una teoría. (p.60).*

Para finalizar el ultimo método a utilizar es el analítico, por la descomposición que se ha realizado a la principal normativa de Riesgo Operativo, se ha tomado lo señalado por Bernal (2003) respecto al método analítico quien menciona: *"Este proceso cognoscitivo consiste en descomponer un objeto de estudio, separando cada una de las partes del todo para estudiarlas en forma individual"* (p.60).

3.4. Población y Muestras

Es necesario aclarar que en el presente proyecto no es aplicable la selección de una población, ni una muestra, para el trabajo únicamente se ha coordinado la entrevista con un experto en riesgos el Ing. Jorge Dilón , cuyo último cargo hasta marzo del 2017 fue de Gerente General de la Calificadora de Riesgos "Sociedad Calificadora Latinoamericana SCR".

3.5. Diseño Metodológico

Tabla 1

Diseño Metodológico

Objetivos Específicos	Tipo de Investigación	Métodos	Técnicas	Instrumentos	Observaciones
Diagnosticar la situación actual de la Administración de Riesgo Operativo en la Cooperativa de Ahorro y Crédito Atuntaqui Ltda.	Documental Descriptiva	Deductivo Inductivo	Observación Directa Recolección de información Entrevista Revisión documental	Cuestionario estructurado con preguntas abiertas y cerradas Grabadora Libreta de Notas	Para el cumplimiento del primer objetivo la observación directa, recolección de la información, entrevistas y revisiones documentales permitirán conocer la situación actual de la COAC Atuntaqui en lo que concierne a la Administración de Riesgo Operativo.
Analizar la aplicación de las Normas Generales para las Instituciones del Sistema Financiero referentes a la gestión del Riesgo Operativo.	Documental Descriptiva	Deductivo Inductivo	Revisión documental	Libros físicos y digitales	A través de una minuciosa revisión documental de toda la información a la mano sobre la gestión de riesgos, específicamente del Riesgo Operativo, permitirá conocer a fondo métodos que permitan analizar de forma eficaz los riesgos operativos en la COAC Atuntaqui.
Desarrollar la Metodología de cálculo para medir los niveles de Gestión de Riesgo Operativo.	Cualitativa Cuantitativa	Analítico	Organización de información	Microsoft Excel	Finalmente el último capítulo establece la metodología a aplicar en la COAC Atuntaqui para conocer y evaluar el estado actual de al Administración de Riesgo Operativo.

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda.

3.6. Procedimiento

Para la ejecución de los objetivos, los procedimientos a realizar van a ser los siguientes:

- Para Diagnosticar la situación actual de la institución referente a la Administración de Riesgos Operativos, la revisión de los informes emitidos por las empresas calificadoras de Riesgos es esencial, porque estas instituciones realizan un estudio similar al que se pretende evaluar, con la diferencia que estas empresas abarcan toda la Administración Integral de Riesgos. De igual manera se analizará los informes de Auditoria Externa en la parte referente a la Administración de Riesgos y verificar el nivel y la importancia que le otorgan al Riesgo Operativo.
- De igual manera es necesario analizar cómo está la Cooperativa frente a la competencia, esto es posible a través del análisis comparativo que otorga la SEPS, en sus boletines mensuales.
- Para la consecución del segundo objetivo es necesario obtener toda la normativa respecto a la Administración de Riesgos, específicamente en la parte referente al Riesgo Operativo, existe normativa emitida por la Superintendencia de Bancos y por la Superintendencia de Economía Popular y Solidaria en lo referente al ámbito nacional, normativa internacional o base legal para el Riesgo se encuentra en los tratados de Basilea y en la ISO 31000. Se verificará que la Cooperativa cumpla los requisitos establecidos en la normativa, y de no ser el caso analizar los proyectos necesarios para su cumplimiento. Con estas bases la información de libros, revistas, artículos científicos complementará el entendimiento y la comprensión de la correcta Administración del Riesgo Operativo e identificar que pueden hacer los administradores de Riesgos para evaluar el estado actual dentro de las instituciones.
- Finalmente para poder desarrollar la metodología la clasificación y análisis minucioso de cada norma en secciones, factores o partes y establecer el peso o la importancia de cada uno de ellos. Por cada factor o sección se establecerá cuestionarios que permitan definir el cumplimiento de lo requerido por la normativa y en los casos que no se cumpla proponer proyectos de cumplimiento a corto o largo plazo. Con los resultados se establecerá una hoja consolidad o resumen con una calificación que permita entender el estado actual del sistema de Administración de Riesgo Operativo. Con estos resultados se deberá proponer conclusiones y recomendaciones de Administración de Riesgo Operativo.

3.7. Técnicas e instrumentos de investigación

Una técnica muy indispensable en cualquier tipo de investigación es la observación directa, Tamayo (2003) indica*: "Es aquella en la cual el investigador puede observar y recoger datos mediante su propia observación"* (p. 183), con esta técnica se podrá identificar a manera de percepción el grado de conocimiento del riesgo operativo que tienen los colaboradores de la entidad, estado de equipos tecnológicos, equipos y muebles de oficina que forman parte del ambiente laboral.

Posteriormente se debe realizar una observación al área de Riesgos, identificar el número de personas que laboran en el área, características, comportamiento, grado de conocimiento sobre el tema y la capacidad del principal responsable del área para tomar decisiones en la institución.

Para poder partir con cualquier proyecto es importante la información que se va a manejar, una vez identificado la documentación base e información necesaria, a través de un control que permita identificar el cumplimiento detallado que cada requerimiento necesario para una correcta administración de riesgos a través de procesos claros, que permita seguir una secuencia ordenada, tal y como Lara (2012) menciona:

> *El control trae muchos beneficios en los negocios por lo que invertir en él, lo convierte en una acción estratégica de gran importancia. En lo financiero genera ahorros al promover eficiencia operativa, en lo administrativo genera información de mayor calidad para la toma de decisiones, en materia de salvaguarda del patrimonio empresarial, reduce la posibilidad de ser víctimas de pérdidas por fraude al disminuir las oportunidades de los perpetradores, entre otros beneficios. (p.23)*

Una de las partes más esenciales en los proyectos es la culminación y la identificación de conclusiones y recomendaciones que permitan una mejora continua de los procesos y procedimientos realizados actualmente, haciendo énfasis en su aplicación y beneficios para la entidad. Para la mejora continua de cualquier metodología implementada, la capacitación que pueda recibir el personal de determinada área es indispensable para el fortalecimiento de los conocimientos, para Chiavenato (2007) la capacitación es el proceso educativo a corto plazo aplicado de manera sistemática y organizada, por medio del cual las personas adquieren conocimientos, desarrollan habilidades y competencias en función de objetivos definidos…(p. 386).

Una técnica indispensable es la recolección de información, tal y como Cesar Bernal lo afirma: "*Un aspecto muy importante en el proceso de una investigación tiene relación con la obtención de la información, pues de ello dependen la confiabilidad y validez del estudio. Obtener información confiable y valida requiere cuidado y dedicación*" (p.191).

Consecuentemente es necesario obtener información de expertos, quienes apoyados de la experiencia aportan de manera sustancial a la investigación, por su parte Cesar Bernal define a la entrevista como:

> *Una técnica orientada a establecer contacto directo con las personas que se consideren fuente de información. A diferencia de la encuesta, que se ciñe a un cuestionario, la entrevista, si bien puede soportarse en un cuestionario muy flexible, tiene como propósito obtener información más espontánea y abierta. Durante la misma, puede profundizarse la información de interés para el estudio. (p. 194).*

Parte fundamental de toda investigación es la revisión de documentos bibliográficos, debido a que una amplia gama de libros, artículos científicos, revistas, sobre un mismo tema permiten ampliar la definición respecto a un aspecto en específico, inicialmente se ha establecido el proyecto en base a un tipo de investigación descriptiva. Para Cesar Bernal *"la investigación descriptiva se soporta principalmente en técnicas como la encuesta, la entrevista, la observación y la revisión documental"* (p. 113).

Los instrumentos de investigación utilizados, permitieron conocer de forma clara y detallada las bases fundamentales para poder sustentar la propuesta que permite solucionar el problema planteado, un cuestionario con preguntas claves, una grabadora que permitió recabar la información brindada por el experto, más la libreta de notas y toda la documentación física y digital, fueron instrumentos indispensables para poder obtener los resultados proyectados.

Para poder concluir y presentar la propuesta definitiva, es indispensable organizar toda la información recabada en la metodología propuesta, brindando un orden y secuencia cronológica que permita entender el proceso establecido. Hernández Sampieri, Fernández Collado, & Baptista Lucio (2010) exponen: *"Dado el amplio volumen de datos, éstos deben encontrarse muy bien organizados. Asimismo, debemos planear qué herramientas vamos a utilizar (hoy en día la gran mayoría de los análisis se efectúa mediante la computadora, al menos un procesador de textos)"* (p.444).

3.8. Resultados esperados (Impactos)

El presente proyecto tiene como objetivo aplicar un enfoque cuantitativo y cualitativo para evaluar el nivel de Administración de Riesgo Operativo, y así identificar los avances y mejorar implementadas en la gestión, identificando fortalezas y debilidades.

3.8.1. En lo económico-social

Al abarcar el aspecto social la Cooperativa Atuntaqui la cual es una entidad de intermediación financiera, dentro de los objetivos institucionales se encuentra la responsabilidad social, debido a que se trabaja con dinero de los socios, por lo tanto una administración correcta del Riesgo Operativo salvaguarda los intereses de los socios.

El aspecto económico es el principal tema de análisis, debido a que se pretende contar con un enfoque cuantitativo que permitirá a la entidad disminuir o controlar la pérdida financiera ocasionada por los impactos generados por eventos de Riesgo Operativo afectando a la rentabilidad institucional.

3.8.2. En lo cultural

La idea de este proyecto es poder crear una cultura de una correcta administración de riesgos en la entidad, debido a que por lo general las personas no dan la importancia a los riesgos que pueden traer consigo la omisión de procesos o la realización de procesos incorrectos o indebidos, el impacto que trae consigo a la entidad y por ende a ellos como originadores.

3.8.3. En lo Metodológico

Referente al impacto metodológico, al investigar nuevas técnicas de análisis, nuevos métodos de cálculo van a permitir desarrollar metodologías estandarizadas que podrán ser aplicadas en cualquier tipo de entidad financiera; permitiendo contar con un documento que permita autoevaluar la gestión de riesgos.

Se puede concluir que los métodos, técnicas e instrumentos utilizados en la presente investigación, permitieron construir la metodología planteada en la propuesta, una vez que se aplique a la COAC Atuntaqui solventará el problema planteado.

CAPÍTULO IV

4 ANALISIS E INTERPRETACION DE RESULTADOS

En el presente capítulo se pretende analizar los resultados arrojados por el diagnóstico realizado de manera inicial a la Administración de Riesgo Operativo en la COAC. Atuntaqui.

Tomando como base el primer objetivo específico que menciona: Diagnosticar la situación actual de la Administración de Riesgo Operativo en la Cooperativa de Ahorro y Crédito Atuntaqui Ltda. y el segundo objetivo específico que menciona: Analizar la aplicación de las Normas Generales para las Instituciones del Sistema Financiero referentes a la gestión del Riesgo Operativo.

Para su cumplimiento se ha previsto realizar el análisis de los siguientes documentos:

Tabla 2

Documentos Normativos

Informe de Calificación Riesgos año 2014 empresa Microfinanzas Rating.
Informe de Calificación Riesgos año 2015 Sociedad Calificadora de Riesgos
Informe de Calificación Riesgos año 2015 Sociedad Calificadora de Riesgos
Afiche de calificación ultimo año 2016 de forma trimestral
Informe de Auditoria Externa del año 2016
Análisis de Boletines mensuales SEPS
Análisis de Calificaciones de Riesgo cooperativas segmento 1 SEPS.
Entrevista realizada al Ing. Jorge Dilón Gerente Calificadora de Riesgos.

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

4.1. Informe de Calificación Riesgos año 2014 empresa Microfinanzas Rating.

Microfinanzas Rating es una empresa de calificación de Riesgo que calificó a la COAC. Atuntaqui desde el año 2012, 2013 y 2014, y en sus informes de Calificación respecto a la Administración de Riesgo Operativo indicaba: Con respecto a riesgo operativo, la Cooperativa ha desarrollado internamente una herramienta de reporte (SARO), el proceso se encuentra automatizado por medio del levantamiento de eventos desde el Service Desk.

Respecto al Riesgo Operativo no realizaba mayor análisis o evaluación en los informes de calificación trimestrales.

4.2. Informe de Calificación Riesgos año 2015 y 2016 Sociedad Calificadora de Riesgos

A partir del año 2015, 2016 por normativa la COAC. Atuntaqui tuvo que cambiar de empresa Calificadora de Riesgos, y contrató los servicios de la Sociedad Calificadora de Riesgos Latinoamericana, la cual en sus informes sobre el Riesgo Operativo realizaba un análisis más profundo enfocado en el siguiente resumen:

- A la fecha Cooperativa de Ahorro y Crédito Atuntaqui Ltda., tiene definido sus macro procesos, procesos, subprocesos y procedimientos o actividades, los cuales registran los cambios y las actualizaciones que se realizan y los plasman en el informe, en el que se define la criticidad de los procesos levantados.
- Cabe indicar que la institución cuenta con un manual de riesgos que por norma se actualiza al menos cada dos años y que en el trimestre en análisis muestra revisiones que han sido puestas a consideración del Consejo de Administración para su aprobación.
- A la misma fecha se lleva el registro de eventos apoyado en la herramienta S.A.R.O., los cuales son analizados y según se informa tratados de forma oportuna. Se comunica también de una continua alimentación con los eventos de riesgo operativo, lo cual se ve evidenciado por los reportes indicados en el informe de riesgos.
- La institución sigue alimentando al sistema de forma semiautomática, ya que dentro del cual se registran automáticamente los eventos de riesgos registrados por la herramienta service desk y otros son ingresados de forma manual.
- Los informes y reportes internos emitidos por la Unidad de Riesgos presentados al Comité de Administración de Riesgos, así como la máxima instancia de administración de la institución, -registrados en las actas de las sesiones correspondientes-, constituyen la evidencia de los resultados de la gestión de la administración del riesgo operativo.
- Se informa de un permanente levantamiento de los eventos y de los factores de riesgo operacional por parte de la Unidad de Riesgos, y su reportamiento al Comité de Administración de Riesgos Integrales de manera mensual, los cuales en el trimestre se dieron por bloqueos de clave y errores en caja, reversos de abonos de crédito, depósitos y retiros.

- La Administración Integral de Riesgos se encuentra actualizada en función de la última resolución emitida por la Junta de Política y Regulación Monetaria y Financiera No. 128-2015-F; siendo el mismo aprobado por el CAIR y por el Consejo de Administración.

A pesar de que en el resumen identificaba puntos relevantes a la Administración de Riesgo Operativo en la cooperativa Atuntaqui el análisis realizado por esta empresa es más minucioso y presentó las siguientes observaciones:

- En lo que respecta al riesgo legal, el informe se limita a indicar los avances que tienen los procesos legales, sin que se observe una evaluación del riesgo inmerso en los mismos ni su probabilidad de impacto y pérdida esperada.
- Se observa un análisis con mayor profundidad de los eventos de riesgo sin embargo, es recomendable que tanto los informes de la Unidad de Riesgos como los del CAIR presente un seguimiento de los eventos de riesgo reportados en meses anteriores para conocer el estatus de las acciones tomadas. Adicional a lo anterior, se sugiere que se presente un detalle del número de veces que se ha presentado un evento de riesgo.
- No se observar una aplicación de metodologías para administrar los riesgos de servicios provistos por terceros, particularmente de aquellos identificados como críticos.
- No maneja un Sistema de Riesgo Operativo y herramientas complementarias que permite realizar un monitoreo constante de la exposición al Riesgo Inherente y Riesgo Residual.
- En lo que respecta al riesgo legal, el informe se limita a indicar los avances que tienen los procesos legales, sin que se observe una evaluación del riesgo inmerso en los mismos ni su probabilidad de impacto y pérdida esperada.

Respecto a ciertos aspectos se indicó a la empresa calificadora de Riesgos los respaldos correspondientes, pero se dió a conocer a la Cooperativa Atuntaqui que necesita fortalecer ciertos aspectos que le permitan medir, y cuantificar el nivel de gestión respecto a la Administración de Riesgo Operativo.

4.3. Afiche de calificación ultimo año 2016 de forma trimestral

El último afiche de calificación otorga una calificación A; que significa: 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 superara 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.

4.4. Informe de Auditoria Externa del año 2016

Respecto a Riesgo Operativo se realizan los siguientes análisis:

- Existencia de objetivos institucionales
- Observación de leyes, normas y reglamentaciones vigentes.
- Contar con planes de contingencia
- Definición de procesos administrativos y operativos claros
- Contar con sistemas de información y tecnológicos

Finalmente explica sobre la situación general de la cooperativa sobre la administración de Riesgo de acuerdo a la resolución 128-2015-F Y 129-2015-F

La empresa Auditora Externa realizó la evaluación con una persona experta en Riesgo, para lo cual respecto a Riesgo Operativo acotó que sería importante conocer el grado de cumplimiento o nivel de gestión, haciendo hincapié que antes no se daba un peso o ponderación significativa al Riesgo Operativo, pero en la actualidad el Riesgo Operativo es un tema que está teniendo mayor importancia debido a los factores que lo conforman.

4.5. Análisis de Boletines mensuales SEPS

La Superintendencia de Economía Popular Solidaria mensualmente emite Boletines mensuales los cuales contienen:

- Índice
- Introducción
- Estados Financiero
- Resultados del Ejercicio
- Clasificación de la cartera
- Ranking
- Indicadores Financieros

Estos boletines nos permiten conocer la situación actual de la Cooperativa Atuntaqui frente a las demás entidades del segmento 1, que contiene a las cooperativas de ahorro y crédito más grandes del Ecuador. A pesar que este análisis es un análisis financiero, se debe entender que una correcta administración de riesgo operativo permitirá que las entidades reflejen mejores resultados, porque un mal análisis de la respuesta ante un evento de riesgo operativo puede generar pérdidas económicas a la entidad, y por ende resultados desfavorables frente a la competencia. Referente a los resultados de las 25 cooperativas financieras que conforman el segmento 1 la Cooperativa Atuntaqui se encuentra en las siguientes posiciones respecto las diferentes cuentas con corte a enero del 2017:

Tabla 3

Ranking Cooperativas

Cuenta Contable	**Posición**
Activos	14
Pasivos	14
Patrimonio	18
Inversión Bruta	15
Cartera Bruta	14
Depósitos a la vista	16
Depósitos a plazo	15
Capital Social y reservas	18
Resultados	8

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

De un total de 25 cooperativas la Cooperativa se encuentra en las posiciones indicadas, se puede verificar que existen otras entidades con mejores resultados, por lo tanto existen algunas estrategias por mejorar que permitirán alcanzar los resultados propuestos por la entidad.

4.6. Análisis de Calificaciones de Riesgo cooperativas segmento 1 SEPS.

En el cuadro indicado, se puede verificar la Calificación de Riesgos de las Cooperativas, y se detalla que la máxima calificación es AA+, lo que significa que actualmente existe muchos indicadores que las cooperativas, incluso las más grandes no cumplen respecto a la Administración de Riesgos, por lo tanto es necesario dar énfasis y demostrar que correctos

procesos y procedimientos permitirán mejorar la calificación de riesgos en para las cooperativas de ahorro y crédito.

Tabla 4

Calificación de Riesgo Cooperativas

COOPERATIVAS	CALIFICACION	EMPRESA CALIFICADORA
CACPECO	AA+ / AA+	BANK WATCH RATINGS / CLASS INTERNATIONAL RATING S.A.
COOPROGRESO	AA	CLASS INTERNATIONAL RATING S.A.
ANDALUCIA	AA-	SOC.CAL.RIESGO LATINOAMERICANA SCRL S.A
JUVENTUD ECUATORIANA PROGRESISTA	A+	SOC.CAL.RIESGO LATINOAMERICANA SCRL S.A
SAN FRANCISCO	A+	PCR PACIFIC S.A
EL SAGRARIO	A+	SOC.CAL.RIESGO LATINOAMERICANA SCRL S.A
COAC DE LA PEQUEÑA EMPRESA DE PASTAZA LTDA.	A+/A+	MICROFINANZA RATING S.A. /CLASS INTERNATIONAL RATING S.A
ATUNTAQUI	A	SOC.CAL.RIESGO LATINOAMERICANA SCRL S.A
JARDIN AZUAYO	A/A	BANK WATCH RATINGS / MICROFINANZA RATING S.A.
RIOBAMBA	A	MICROFINANZA RATING S.A.
OSCUS	A	SOC.CAL.RIESGO LATINOAMERICANA SCRL S.A
23 DE JULIO	A	PCR PACIFIC S.A.
ALIANZA DEL VALLE	A	SOC.CAL.RIESGO LATINOAMERICANA SCRL S.A
TULCAN LTDA.	A	SOC.CAL.RIESGO LATINOAMERICANA SCRL S.A
MEGO	A-	PCR PACIFIC S.A.
PABLO MUÑOZ VEGA	A-	SOC.CAL.RIESGO LATINOAMERICANA SCRL S.A
CACPE BIBLIAN	A-	PCR PACIFIC S.A.
POLICIA NACIONAL	A-	SOC.CAL.RIESGO LATINOAMERICANA SCRL S.A
SAN JOSE LTDA	A-	SOC.CAL.RIESGO LATINOAMERICANA SCRL S.A
SANTA ROSA	BBB+	SOC.CAL.RIESGO LATINOAMERICANA SCRL S.A
MUSHUC RUNA	BBB-	SOC.CAL.RIESGO LATINOAMERICANA SCRL S.A
29 DE OCTUBRE	BB+/BB+	BANK WATCH RATINGS / CLASS INTERNATIONAL RATING S.A.
CAMARA DE COMERCIO DE AMBATO	BB	MICROFINANZA RATING S.A.
SERVIDORES PUBLICOS DEL MINISTERIO DE EDUCACION Y CULTURA	BB-	MICROFINANZA RATING S.A.
PILAHUIN TIO LTDA	No tiene calificaciòn	

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

4.7. Entrevista realizada al Ing. Jorge Dilón Gerente Calificadora de Riesgos Sociedad Latinoamericana.

El Ing. Jorge Dilón fue el gerente de la empresa Calificadora de Riesgos Sociedad Latinoamericana hasta el mes de marzo del 2017. La entrevista constó en las siguientes preguntas:

- ¿En qué consiste la actividad de las empresas Calificadora de Riesgos?
- ¿Cómo ve la actual Administración de Riesgos de la COAC Atuntaqui?

- ¿Qué ponderación o peso le da al Riesgo Operativo?
- ¿Qué recomendación podría dar respecto a la administración del Riesgo Operativo en la COAC Atuntaqui?
- ¿Cuáles son las bases para una correcta Administración de Riesgo Operativo?
- ¿Qué normas son indispensables analizar para interpretar de manera correcta la Administración del Riesgo Operativo?

A manera resumida se presenta el criterio del Ing. Jorge Dilón para las preguntas realizadas, vía telefónica: Mencionado experto acotó que las empresas de Calificación de Riesgos tienen como objetivo evaluar la administración de riesgos de entidades financieras, compañías, sociedades anónimas, empresas de mercado de valores, con el objetivo de establecer una calificación que permita conocer y evaluar de forma rápida la seguridad y confianza de una entidad. Actualmente la COAC Atuntaqui es una de las cooperativas más grandes del Ecuador, pero al igual que muchas entidades no han dado la debida importancia al Riesgo Operativo, y menciona y recomienda que se debería estudiar y analizar de forma detallada todas las resoluciones, normativa, documentos que existen sobre Riesgo Operativo, pero insiste en la revisión a detalle del 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 (incluido con resolución No JB-2005-834 de 20 de octubre del 2005).

En base a este análisis se puede acotar que la entidad cumple de manera parcial lo indicado respecto al cumplimiento de las normas emitidas por los organismos de control.

Por parte de Auditoría Interna existen recomendaciones respecto a la aplicación de políticas para el control de servicios provistos por terceros y de orden legal y se puede identificar que a pesar de no existir recomendaciones explicitas a la Administración Integral de Riesgos Operativo, al no conocer de forma cualitativa ni cuantitativa su nivel de gestión, es imposible demostrar de forma contundente el grado de gestión y mejora en el manejo de la administración riesgo operativo.

Al realizar un análisis frente a las interrogantes de la investigación, se puede definir que la situación actual de la Administración de Riesgos de la COAC Atuntaqui, no cumple a cabalidad con lo requerido en la normativa expedida por el Organismo de Control, debido a

que la aplicación de las normas generales expedidas para las instituciones financieras referente a la gestión de Riesgo Operativo son cumplidas de manera parcial, de acuerdo a los requerimientos o necesidades de la entidad, pero al no contar con una metodología de evaluación se desconoce cuál es el nivel exacto referente a la Administración de Riesgo Operativo, ocasionando que se desconozca el beneficio alcanzado al implementar una estrategia, y de igual manera el impacto que puede ocasionar el desconocimiento o la no aplicación de la normativa.

CAPÍTULO V

5. PROPUESTA

En el siguiente capítulo se realiza una explicación a la metodología propuesta para evaluar el Sistema de Administración de Riesgo Operativo aplicado en la Cooperativa de Ahorro y Crédito Atuntaqui Ltda., para poder cualificar y cuantificar el nivel de Administración de Riesgo Operativo, por lo tanto se detalla de forma específica la metodología a aplicar.

5.1. Flujogramas

Inicialmente se presenta el flujograma que explica la metodología aplicada.

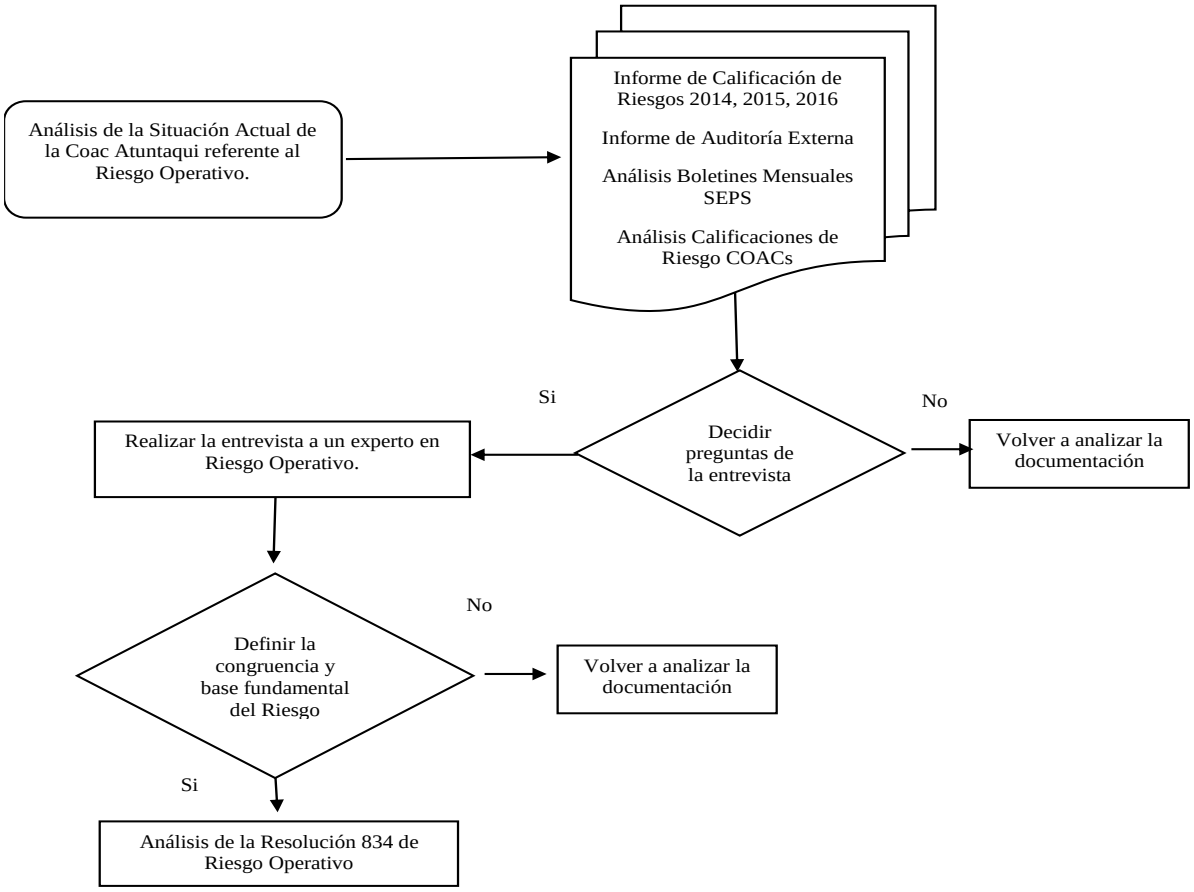
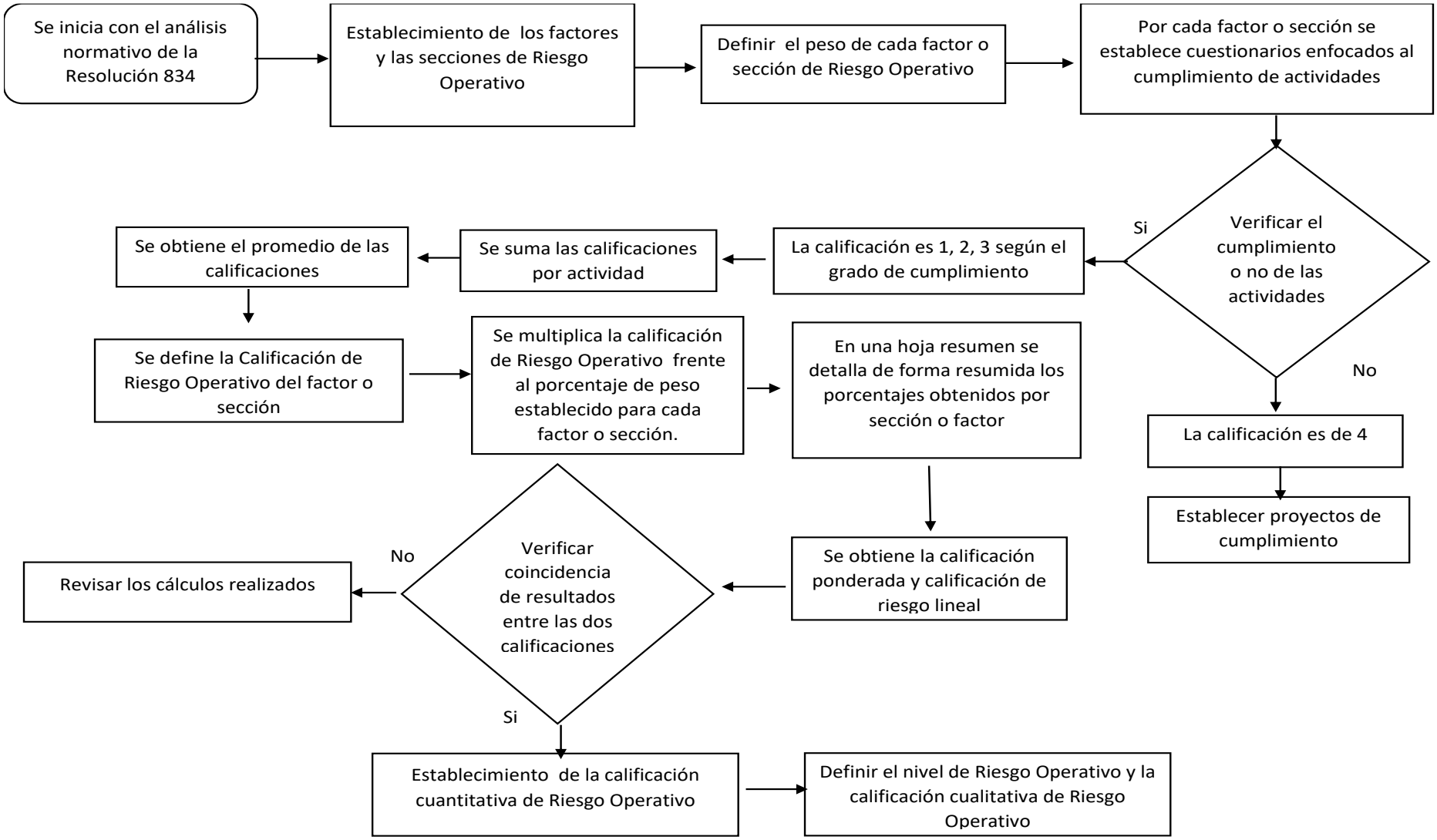


Figura 1 Metodología aplicada

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda



Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

5.2. Metodología de Evaluación

1. Tomando como base y fundamentos toda la información recabada de Riesgo Operativo, principalmente el 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 (incluido con resolución No JB-2005-834 de 20 de octubre del 2005), y con la ayuda referente a la opinión de expertos sobre Riesgo Operativo se pudo definir las secciones y factores que conforman el análisis de Riesgo Operativo, las cuales se detallan a continuación:

Tabla 5

Secciones y factores de Riesgo

N°	SECCION Y FACTORES
1	PERSONAS
2	PROCESOS
3	TECNOLOGIA DE LA INFORMACION
4	EXTERNO Y TERCEROS
5	SEGURIDAD INFORMACIÓN
6	ADMINISTRACION INTEGRAL DE RIESGOS
7	ALTA DIRECCION
8	CONTINUIDAD DE NEGOCIOS

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

2. Posterior al análisis es indispensables establecer el peso de cada factor y sección, para lo cual basado en los cuatro factores que conforman el Riesgo Operativo se les otorgará la calificación del 10%, y a las secciones de Seguridad de la Información, Administración Integral de Riesgos, la Alta Dirección o Gobierno Corporativo y la Continuidad del Negocio según los impactos que puede acarrear a una institución su falta de aplicación se les ha asignado el porcentaje del 15%.

Tabla 6

Pesos Factores y Secciones de Riesgo

N°	FACTORES y SECCIONES	Porcentaje
1	PERSONAS	10%
2	PROCESOS	10%
3	TI	10%
4	EXTERNO Y TERCEROS	10%
5	SEGURIDAD INFORMACIÓN	15%
6	AIR	15%
7	ALTA DIRECCION	15%
8	CONTINUIDAD DE NEGOCIOS	15%
TOTAL		100%

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

3. Por lo tanto en cada factor y sección se establecerá un cuestionario de cumplimiento enfocado en los siguientes parámetros:

   a) Que se busca verificar con el cuestionario a realizar

   b) Establecer las actividades requeridas

   c) Por cada actividad se establece la calificación de Riesgos basado en los siguientes ítems:

Tabla 7

Calificaciones al cumplimiento

n/a (0)	No aplica a la entidad
cumple (1)	Se cumple en un 100% la actividad requerida
satisfactorio (2)	Hay un cumplimiento satisfactorio del mismo, no a un 100%, pero si existe un porcentaje avanzado de cumplimiento.
Parcialmente (3)	Existe un cumplimiento parcial o se está implementando el mismo en la entidad.
No cumple (4)	No cumple la entidad.

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

d) Finalmente se establecerá de todos los ítems una suma por actividad.

e) Si la respuesta es “No Cumple”, como acción de mitigación y mejoramiento se propone que el área evaluada proponga un proyecto para dar cumplimiento a la actividad con la cual no se está cumpliendo, todo esto basado en los siguientes parámetros:

- Porcentaje de avance de implementación
- Fecha inicio y fin del proyecto.
- Área Responsable
- Referencia

f) Se detalla la normativa exigible que se está cumpliendo o se necesita cumplir.

A continuación se indica la matriz de cumplimiento y calificación de actividades por cada factor y sección.

Tabla 8

Matriz de Cumplimiento

SECCION										
FACTOR										normativa
	n/a	Cumple	satisfactorio	parcialmente	No cumple	TOTAL	Si la respuesta es "No Cumple", completar datos del proyecto			
ACTIVIDAD	0	1	2	3	4		Porcentaje avance proyecto	Fechas inicio y fin	Área responsable	Referencia

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

SECCION										
FACTOR										normativa
	n/a	cumple	satisfactorio	Parcialmente	No cumple	TOTAL	Si la respuesta es "No Cumple", completar datos del proyecto			
ACTIVIDAD	0	1	2	3	4		Porcentaje avance proyecto	Fechas inicio y fin	Área responsable	Referencia
Actividad 1	0					1				
Actividad 2		1				1				
Actividad 3			2			2				
Actividad 4				3		3				
Actividad 5					4	4				
total	0	1	2	3	4	=(0+1+2+3+4) = 10				

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

4. Dentro del análisis de cada factor o sección, se realizará la sumatoria de los ítems por cada actividad, tal y como se detalla a continuación:

   NOTA: Esta calificación está sujeta a validación con los respectivos documentos.

5. Para establecer la calificación de Riesgo se saca el promedio de los totales de cada actividad, en el ejemplo seria promedio de (0,1,2,3,4); que da un resultado de “2”.

6. Una vez establecido la Calificación de Riesgo es necesario establecer a que nivel de Riesgo pertenece, por lo tanto basado en el número de ítems de calificación (que es 5 items), se ha procedido a establecer cinco niveles de calificación.

Tabla 9

Niveles de Riesgo

Nivel uno	Riesgo bajo
Nivel dos	Riesgo medio bajo
Nivel tres	Riesgo medio
Nivel cuatro	Riesgo medio alto
Nivel cinco	Riesgo alto

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

7. Para ponderar el rango de cada nivel de riesgo, se parte que cuando una actividad o requisito no aplica para la entidad la calificación es 0 (no existe riesgo), si la entidad cumple con la actividad o el requisito la calificación es 1, si la entidad cumple de forma satisfactoria la calificación es 2, si se cumple parcialmente es 3, y si no se cumple la calificación es 4.

De igual manera el valor mínimo del rango de riesgo será 0 que quiere decir que no existe riesgo, y el valor máximo del rango de riesgo será 4, que equivale a una calificación de riesgo alto que puede obtener una entidad que no cumple con el requisito.

Tabla 10

Explicación niveles de Riesgo

Valor Mínimo Nivel 1 = 0	(Debido a que si el requerimiento no aplica para la entidad, no existe riesgo)
Valor Máximo Nivel 1 = 1	(Debido a que si la entidad cumple con el requerimiento es 1, y por ende el nivel de riesgo es bajo)
Valor Mínimo Nivel 2 = 1,01	Puede que la entidad cumpla, pero no al 100%, por lo tanto el riesgo es medio bajo
Valor Máximo Nivel 2 = 1,75	Puede que la entidad cumpla, pero no al 100%, por lo tanto el riesgo es medio bajo
Valor Mínimo Nivel 3 = 1,76	La entidad cumple con lo requerido aproximadamente en un 50%, no puede justificar a un 100% el cumplimiento, por lo tanto el riesgo es medio.

Valor Máximo Nivel 3 = 2,5	La entidad cumple con lo requerido aproximadamente en un 50%, no puede justificar a un 100% el cumplimiento, por lo tanto el riesgo es medio.
Valor Mínimo Nivel 4 = 2,51	La entidad ha iniciado posibles estrategias de cumplimiento, pero que no logran cubrir el impacto del riesgo, por lo tanto el riesgo es medio alto
Valor Máximo Nivel 4 = 3,25	La entidad ha iniciado posibles estrategias de cumplimiento, pero que no logran cubrir el impacto del riesgo, por lo tanto el riesgo es medio alto
Valor Mínimo Nivel 5 = 3,26	La entidad no cumple con lo requerido, el riesgo es alto
Valor Máximo Nivel 5 = 4	La entidad no cumple con lo requerido, el riesgo es alto

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

Establecimiento de Rangos

Valor Mínimo Nivel 1 = 0

Valor Máximo Nivel 5 = 4

Para establece el rango de los cuatro siguientes niveles se ha aplicado el siguiente razonamiento:

- (Valor máximo Nivel 5 *menos* 1) / (número de niveles sin rango)

  = (4 – 1) / 4

  = 3 / 4

  = 0,75 (diferencia entre rangos)

Tabla 11

Rango por nivel de Riesgo

		Rango Mínimo	Rango Máximo
Nivel uno	Riesgo bajo	0	1
Nivel dos	Riesgo medio bajo	= Rango máximo nivel uno + 0,01	= Rango máximo nivel uno + 0,75
Nivel tres	Riesgo medio	= Rango máximo nivel dos + 0,01	= Rango máximo nivel dos + 0,75
Nivel cuatro	Riesgo medio alto	= Rango máximo nivel tres + 0,01	= Rango máximo nivel tres + 0,75
Nivel cinco	Riesgo alto	= Rango máximo nivel cuatro + 0,01	4

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

Por lo tanto la tabla de niveles de Riesgo es la siguiente:

Tabla 12

Nivel y calificación de Riesgo

0	1,00	bajo
1,01	1,75	medio bajo
1,76	2,50	medio
2,51	3,25	medio alto
3,26	4,00	alto

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

8. Una vez establecidos los niveles de Riesgo se procede a evaluar cada factor o sección, y se podría establecer la siguiente tabla, por método de ejemplificación se tomará como que se ha obtenido el mejor puntaje en cada proceso, es decir se ha cumplido con todos los requerimientos, por lo tanto la calificación es 1:

Tabla 13

Ponderación según Pesos de Factores y Secciones

N°	FACTORES y SECCIONES	Porcentaje	Calificación	
1	PERSONAS	10%	1	0,10
2	PROCESOS	10%	1	0,10
3	TI	10%	1	0,10
4	EXTERNO Y TERCEROS	10%	1	0,10
5	SEGURIDAD INFORMACIÓN	15%	1	0,15
6	AIR	15%	1	0,15
7	ALTA DIRECCION	15%	1	0,15
8	CONTINUIDAD DE NEGOCIOS	15%	1	0,15
TOTAL		100%	1	

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

La calificación ponderada por peso = 1 y equivale a un nivel de riesgo bajo

9. Una vez obtenido el la calificación se ha otorgado una calificación de Riesgo en letras según el siguiente detalle:

Tabla 14

Definición Calificación de Riesgo

Nivel Riesgo	Rango Mínimo	Rango Máximo	Riesgo	Calificacion Riesgo
Uno	0	1.00	bajo	A
Dos	1.01	1.75	medio bajo	B
Tres	1.76	2.50	medio	C
Cuatro	2.51	3.25	medio alto	D
Cinco	3.26	4.00	alto	E

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

Tabla 15

Definición a la calificación de Riesgo

Calificación Riesgo	Definición
A	La administración de Riesgo Operativo es muy fuerte y tiene un sobresaliente cumplimiento de la normativa, se ha establecido claros controles de mitigación del riesgo operativo. Si existe debilidad o vulnerabilidad en algún aspecto de la administración de riesgo operativo, ésta se mitiga enteramente con las fortalezas de la organización.
B	Se considera claramente que existe una buena Administración de Riesgo Operativo, con un cumplimiento adecuado de la normativa de riesgos, aunque son evidentes algunos obstáculos menores, éstos no son serios y/o son perfectamente manejables a corto plazo.
C	La Administración de Riesgo Operativo sugiere obvias deficiencias, muy probablemente relacionadas con el incumplimiento de algunos aspectos normativos. Hacia el futuro existe un considerable nivel de incertidumbre en el cumplimiento de los procedimientos para un correcto control del riesgo operativo, pero con la propuesta de proyectos o actualizaciones se puede alcanzar las mejoras a un corto o largo plazo.
D	La institución tiene considerables deficiencias en la Administración de Riesgo Operativo, que probablemente incluyen dificultades en la estructura del área encargada de su manejo y control; Existe un alto nivel de incertidumbre sobre poder afrontar eventos de riesgo adicionales que puedan presentarse de forma imprevista.
E	No existe una cultura de Administración de Riesgo Operativo, más bien se identifica un asentado desconocimiento e incumplimiento de la normativa de riesgo operativo, exponiendo a la entidad a eventos de riesgo que puedan originar pérdidas econòmicas a la misma.

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

10. Para finalizar se establece una hoja resumen para analizar de forma sintetizada los puntajes obtenidos por cada factor o sección, y finalmente se establece dos calificaciones una de Riesgo Lineal y otra ponderada por peso. Las dos calificaciones deben pertenecer al mismo nivel de Riesgo. (a manera de comprobación)

CALIFICACION DE RIESGO LINEAL.- es el resultado de una tabla generada en una hoja consolidada con todos los factores y secciones, donde se ha aplicado la metodología descrita anteriormente.

CALIFICACION PONDERADA POR PESO.- Es el resultado obtenido del procedimiento establecido, donde posterior al análisis por cada factor sección, se establecía un peso por cada uno, y se procedía a determinar la calificación de riesgo.

5.3. Aplicación metodológica a la COAC Atuntaqui Ltda.

En base a los fundamentos establecidos en la normativa se estableció el análisis de las siguientes secciones y factores:

Tabla 16

Secciones y factores de Riesgo

N°	SECCION Y FACTORES
1	PERSONAS
2	PROCESOS
3	TECNOLOGIA DE LA INFORMACION
4	EXTERNO Y TERCEROS
5	SEGURIDAD INFORMACIÓN
6	ADMINISTRACION INTEGRAL DE RIESGOS
7	ALTA DIRECCION
8	CONTINUIDAD DE NEGOCIOS

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

Para los cuatro factores que conforman el Riesgo Operativo se les otorgará la calificación del 10%, y a las secciones de Seguridad de la Información, Administración Integral de Riesgos, la Alta Dirección o Gobierno Corporativo y la Continuidad del Negocio según los impactos que puede acarrear a una institución su falta de aplicación se les ha asignado el porcentaje del 15%.

Tabla 17

Pesos Factores y Secciones de Riesgo

N°	FACTORES y SECCIONES	Porcentaje
1	PERSONAS	10%
2	PROCESOS	10%
3	TI	10%
4	EXTERNO Y TERCEROS	10%
5	SEGURIDAD INFORMACIÓN	15%
6	AIR	15%
7	ALTA DIRECCION	15%
8	CONTINUIDAD DE NEGOCIOS	15%
TOTAL		100%

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

Se aplicó el cuestionario por cada factor y sección aplicando la siguiente matriz y poder obtener los datos presentados posteriormente.

Tabla 18

Matriz de Cumplimiento

SECCION											
FACTOR	n/a	Cumple	satisfactorio	parcialmente	No cumple	TOTAL	Si la respuesta es "No Cumple", completar datos del proyecto				normativa
ACTIVIDAD	0	1	2	3	4		Porcentaje avance proyecto	Fechas inicio y fin	Área responsable	Referencia	

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

PROCESOS

Como resultado de la evaluación realizada a 18 actividades del factor procesos, se obtuvo una calificación de 2,11 que equivale a un riesgo medio; se recomienda implementar políticas que permitan la identificación de los procesos críticos y el diseño claro de los procedimientos establecidos en los manuales de normalización y estandarización.

Tabla 19

Calificación de Riesgo Procesos

CALIFICACION DE RIESGO	2,11	medio

calificacion	riesgo
0	0
0	0
2,111111111	medio
0	0
0	0

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

PERSONAS

Como resultado de la evaluación realizada a 14 actividades del factor personas, se obtuvo una calificación de 2,07 que equivale a un riesgo medio; se recomienda mejorar los procesos de incorporación y capacitación al personal realizados por parte del área de Talento Humano.

Tabla 20

Calificación de Riesgo Personas

CALIFICACION DE RIESGO	2,07	medio

calificacion	riesgo
0	0
0	0
2,071428571	medio
0	0
0	0

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

TECNOLOGIA DE LA INFORMACION

Como resultado de la evaluación realizada a 32 actividades del factor tecnología de la información, se obtuvo una calificación de 1,97 que equivale a un riesgo medio; se recomienda establecer metodologías para la administración de proyectos enfocadas en la optimización de recursos y la gestión de riesgos, adicionalmente se debe integrar un inventario de la infraestructura tecnológica, identificando ítem, registro, responsables de uso y mantenimiento e incorporar un Plan Operativo de necesidades tecnológicas.

Tabla 21

Calificación de Riesgo TI

CALIFICACION DE RIESGO	1,97	medio

calificacion	riesgo
0	0
0	0
1,96875	medio
0	0
0	0

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

EVENTOS EXTERNOS Y SERVICIOS PROVISTOS POR TERCEROS

Como resultado de la evaluación realizada a 19 actividades del factor eventos externos y servicios provistos por terceros, se obtuvo una calificación de 3,53 que equivale a un riesgo alto; se recomienda establecer un manual de procesos que cumpla con políticas, procesos y procedimientos elaborados y aplicados para selección, calificación y evaluación de los proveedores.

Tabla 22

Calificación de Riesgo Eventos y Servicios Tercero

CALIFICACION DE RIESGO	3,53	alto

calificacion	riesgo
0	0
0	0
0	0
0	0
3,526315789	alto

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

SEGURIDAD DE LA INFORMACION

Como resultado de la evaluación realizada a 21 actividades de la sección seguridad de la información, se obtuvo una calificación de 2,07 que equivale a un riesgo medio; se recomienda establecer un Comité de Seguridad de la Información que realice un seguimiento minucioso a todas las actividades que repercuten en un control y manejo adecuado de la información.

Tabla 23

Calificación de Riesgo Seguridad Información

CALIFICACION DE RIESGO	2,07	medio

calificacion	riesgo
0	0
0	0
2,074074074	medio
0	0
0	0

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

ADMINISTRACION INTEGRAL DE RIESGOS

Como resultado de la evaluación realizada a 21 actividades de la sección Administración Integral de Riesgos, se obtuvo una calificación de 2,38 que equivale a un riesgo

medio; se recomienda establecer procedimientos que engloben las fallas o insuficiencias de orden legal enfocados en los siguientes campos: Actos Societarios, Gestión de Crédito, Operación del giro financiero, Actividades complementarias de las operaciones del giro financiero y Cumplimiento legal y normativo.

Tabla 24

Calificación de Riesgo Administración Integral de Riesgos

CALIFICACION DE RIESGO	2,38	medio

calificacion	riesgo
0	0
0	0
2,380952381	medio
0	0
0	0

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

ALTA DIRECCION

Como resultado de la evaluación realizada a 15 actividades de la sección Alta Dirección, se obtuvo una calificación de 1,87 que equivale a un riesgo medio; es necesario seguir fortaleciendo las funciones del Consejo de Administración, Gerencia, Comité de Riesgos, Área de Riesgos respecto a las actividades de Gestión Integral de Riesgos.

Tabla 25
Calificación de Riesgo Alta Dirección

CALIFICACION DE RIESGO	1,87	medio

calificacion	riesgo
0	0
0	0
1,866666667	medio
0	0
0	0

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

CONTINUIDAD DEL NEGOCIO

Como resultado de la evaluación realizada a 22 actividades de la sección Continuidad del Negocio, se obtuvo una calificación de 2,77 que equivale a un riesgo medio alto; es necesario la formación del Comité de Continuidad del Negocio, con el objetivo que los procesos críticos, tengan estrategias que permitan contar con procesos o procedimientos alternos y contingentes.

Tabla 26

Calificación de Riesgo Continuidad de Negocio

CALIFICACION DE RIESGO	2,77	medio alto

calificacion	riesgo
0	0
0	0
0	0
2,772727273	medio alto
0	0

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

Una vez establecidos los niveles de Riesgo se procedió a evaluar cada factor y sección y se obtuvo los siguientes resultados:

Tabla 27

Ponderación según Pesos de Factores y Secciones Coac Atuntaqui

N°	FACTORES Y SECCIONES	Porcentaje	Puntuación	Calificación
1	PERSONAS	10%	2,07	0,21
2	PROCESOS	10%	2,11	0,21
3	TI	10%	1,97	0,20
4	EXTERNO Y TERCEROS	10%	3,53	0,35
5	SEGURIDAD INFORMACIÓN	15%	2,07	0,31
6	AIR	15%	2,38	0,36
7	RESPON DIRECCION	15%	1,87	0,28
8	CONTINUIDAD DE NEGOCIOS	15%	2,77	0,42
TOTAL		100%		2,33

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

Se establece una hoja resumen para analizar de forma sintetizada los puntajes obtenidos por cada factor o sección:

CALIFICACION DE RIESGO LINEAL.- La Calificación de Riesgos obtenida es de 2,33 que equivale a un nivel de riesgo medio.

CALIFICACION PONDERADA POR PESO.- La Calificación de Riesgos obtenida es de 2,33 que equivale a un nivel de riesgo medio.

CALIFICACION ADMINISTRACION DE RIESGO OPERATIVO COAC ATUNTAQUI.- En base a la calificación de Riesgo que nos permite de definir de forma cuantitativa y cualitativa el nivel de Administración de Riesgo, según la siguiente tabla se obtuvo los siguientes resultados:

Tabla 28

Definición Calificación de Riesgo

Nivel Riesgo	Rango Mínimo	Rango Máximo	Riesgo	Calificacion Riesgo
Uno	0	1,00	bajo	A
Dos	1,01	1,75	medio bajo	B
Tres	1,76	2,50	medio	C
Cuatro	2,51	3,25	medio alto	D
Cinco	3,26	4,00	alto	E

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

Tabla 29

Resultado Calificación Riesgo COAC Atuntaqui

ACTIVIDADES EVALUADAS	0	42	54	46	26	168
TOTAL PUNTAJE	0	42	108	138	104	392
CALIFICACION DE RIESGO LINEAL	2,33			medio		
CALIFICACION PONDERADA POR PESO	2,33			medio		
NIVEL DE RIESGO	cinco					
CALIFCACION ADMINISTRACION RIESGO OPERATIVO COAC ATUNTAQUI	C					
La Administración de Riesgo Operativo sugiere obvias deficiencias, muy probablemente relacionadas con el incumplimiento de algunos aspectos normativos. Hacia el futuro existe un considerable nivel de incertidumbre en el cumplimiento de los procedimientos para un correcto control del riesgo operativo, pero con la propuesta de proyectos o actualizaciones se puede alcanzar las mejoras a un corto o largo plazo.						

Elaborado por el Autor
Fuente: COAC Atuntaqui Ltda

Con la aplicación de la metodología se pudo obtener un conocimiento exacto de la situación actual de la Cooperativa Atuntaqui, debido a que la misma permite conocer el nivel cuantitativo y cualitativo del sistema de Administración de Riesgo Operativo, mencionada metodología obtiene una calificación de 2.33 que equivale a un riesgo medio, otorgándole un nivel "C" de calificación, que significa que la Administración de Riesgo Operativo sugiere obvias deficiencias, muy probablemente relacionadas con el incumplimiento de algunos aspectos normativos. Hacia el futuro existe un considerable nivel de incertidumbre en el cumplimiento de los procedimientos para un correcto control del riesgo operativo, pero con la propuesta de proyectos o actualizaciones se puede alcanzar las mejoras a un corto o largo plazo.

Se puede concluir que la aplicación de la Metodología de Evaluación al Sistema de Administración de Riesgo Operativo en la Cooperativa de Ahorro y Crédito Atuntaqui Ltda., es viable y pertinente, debido a que cumple el objetivo general establecido y solventa el problema identificado inicialmente.

CAPÍTULO VI

6. CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Realizada y aplicada la metodología de evaluación al sistema de Administración de Riesgo Operativo en la COAC Atuntaqui se obtuvo las siguientes conclusiones:

- La Administración de Riesgo Operativo manejada en la Cooperativa de Ahorro y Crédito Atuntaqui Ltda. refleja algunas deficiencias referentes al cumplimiento de ciertos parámetros necesarios para la mitigación de los impactos producidos por eventos de riesgo operativo.
- La Cooperativa de Ahorro y Crédito Atuntaqui no ha cumplido a cabalidad la normativa expedida por los Organismos de Control Nacionales y ciertas normas expedidas por Organismos Internacionales debido a un control limitado por parte de organismos externos a la entidad como empresas Auditoras y Calificadoras de Riesgo.
- Los niveles de gestión de Riesgo Operativo de la Cooperativa Atuntaqui reflejan una calificación de Riesgo de 2,33 que equivale a un nivel de Riesgo Medio y a una calificación "C" que significa que la entidad sugiere obvias deficiencias en la Administración de Riesgo Operativo relacionadas al incumplimiento normativo.

RECOMENDACIONES

Por tal motivo es necesario plantear las siguientes recomendaciones:

- El Área de Riesgos de la COAC Atuntaqui deberá solicitar a la administración capacitaciones por lo menos dos veces al año enfocadas en la Administración de Riesgo Operativo, previo al compromiso de los integrantes de mencionada área que de cada capacitación asistida se presentará el proyecto de mejora respectivo.
- El área de Administración de Riesgo Operativo deberá monitorear diariamente resoluciones emitidas por los organismos de control y supervisión en el campo del Riesgo Operativo, posteriormente se deberá establecer el monitoreo al cumplimiento de mencionadas resoluciones.
- Una vez conocidos los resultados arrojados por la metodología de evaluación, el Área de Riesgos de la COAC Atuntaqui, deberá analizar los puntos a mejorar establecidos en la Hoja Resumen de mencionada metodología, para que en el lapso de un tiempo determinado se establezca los proyectos que permitan cumplir los puntos citados y mejorar la calificación cualitativa y cuantitativa de Administración de Riesgo Operativo.

BIBLIOGRAFÍA

Aguilar, A. S. (2004). *Capacitación y Desarrollo de Personal.* Mexico: Editorial Limusa S.A.

Alvarado Dario y Moran Gabrila. (2010). *Metodos de Investigación.* Pearson.

Areitio Bertolín , J. (2008). *Seguridad de la Información.* España: Paraninfo.

Arizabaleta, E. V. (2004). Concepto. En E. V. Arizabaleta, *Diagnóstico Organizacional: evaluación sistémica del desempeño empresarial en la era digital* (pág. 20). Bogotá: Ecoe Ediciones.

Baez Paz, G. M. (2014). La Metodología de investigación. En G. M. Baez Paz, *Metodología de la investigación* (pág. 43). México: Grupo Editorial Patria.

Bernal, C. (2010). *metodologia de la investigacion* . Pearson educación .

Casares, I. (2013). Administración de los riesgos. En I. Casares, *Proceso de Gestión de Riesgos y Seguros en las Empresas* (pág. 26). Madrid: Molinuevo.

Castillo, M., & Mendoza, A. (2002). Diseño de una Metodología para la Identificación y la Medición del Riesgo Operativo en Instituciones Financieras. *Universidad de los Andes - Facultad de Ingeniería*, 46.

Chiavenato, I. (2007). *Administraciòn de Recursos Humanos.* Colombia: McGraw-Hill.

Cook y Winkle. (2006). *Manual de control interno administrativo.* Los Angeles: Mac Graw Hill.

Costas Santos, J. (2014). *Seguridad Informática.* Madrid: RA-MA.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio , P. (2010). *Metodología de la Investigación.* México D.F.: McGraw-Hill / Interamericana Editores S.A.

Lara, A. (2012). *Toma el Control de tu Negocio.* Mèxico: LID Editorial.

López Parra, M. E. (2004). ¿Cómo Determinar su Riesgo Empresarial? *Revista Escuela de Administración de NegocioS*, 70.

Marín Idárraga, D. A. (2012). Estructura organizacional y sus parámetros de diseño: análisis descriptivo en pymes industriales de Bogotá. *Estudios Gerenciales*, 46.

Marín Idárraga, D. A., & Losada Campos, L. Á. (2015). Estructura organizacional y relaciones inter-organizacionales: análisis. *Estudios Gerenciales*, 90.

Martínez, J. G. (2004). *Planes de contingencia: la continuidad del negocio en las organizaciones.* Madrid: Ediciones Díaz de Santos.

Mejía Delgado, H. (2011). *Gestión integral de riesgos y seguros.* Bogotá: Ecoe Ediciones.

Molina Mateos, J. M. (2000). *Seguridad de la información. Criptología.* Córdoba: El Cid Editor.

Navarro Chávez , J. L. (2014). Conceptos y Definiciones. En J. L. Navarro Chávez, *Epistemología y metodología* (págs. 17-18). Mexico: Grupo Editorial Patria.

Palma Rodríguez, C. (2011). ¿Cómo construir una matriz de Riesgo Operativo? *Ciencias Económicas*, 631.

Pérez Barbeito, J. (2014). Los riesgos financieros internacionales. En J. Pérez Barbeito, *Finanzas internacionales: cómo gestionar los riesgos financieros internacionales* (pág. 199). Santiago de Chile: Universidad de Santiago de Chile.

Prieto Herrera, J. E. (2009). El diagnóstico organizacional. En J. E. Prieto Herrera, *Gestión estratégica organizacional: guía practica para el diagnóstico empresarial* (pág. 22). Bogotá: Ecoe Ediciones.

Rivero, D. S. (2008). *Metodologia de la Investigación* . Shalon.

Roberto Hernandez Sampiere, C. F. (1991). *Metodología de la invesstigación.* Mexico: Mcgraw-Hill.

Rubio Romero, J. C. (2002). *Gestión de la prevención de riesgos laborales.* Madrid: Ediciones Díaz de Santos.

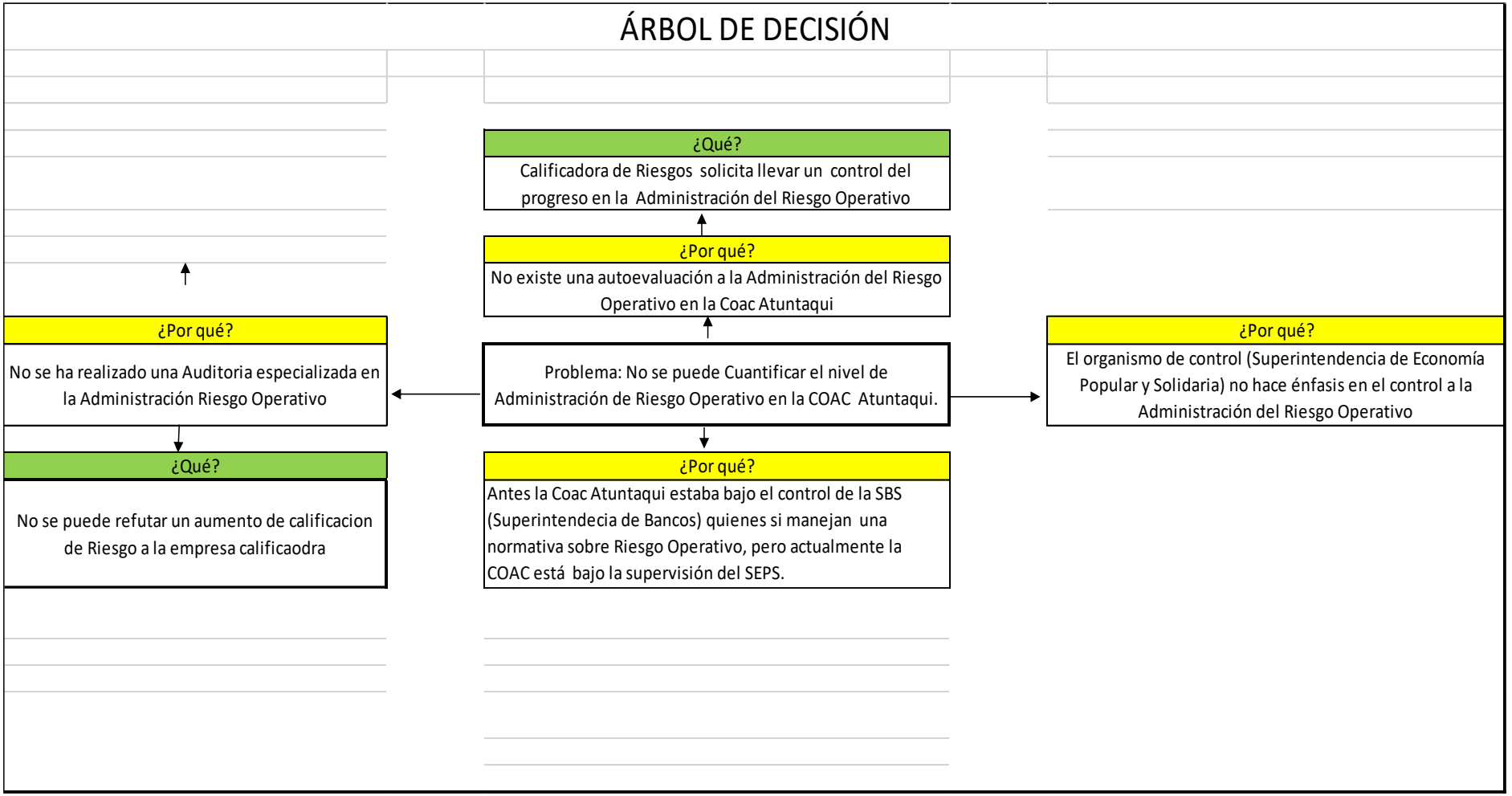
Scaron de Quintero, M. T. (1985). El Díagnóstico Social. En M. T. Scaron de Quintero, *El Díagnóstico Social* (pág. 26). Buenos Aires: Humanitas.

Soto Concha, R. F. (2009). Definiciones. En R. F. Soto Concha, *Diseño de una estructura organizacional, para la empresa Turbomecanica LTDA* (pág. 8). Santiago de Chile.

Tamayo, M. T. (2003). *El proceso de la investigación científica.* Mexico: LIMUSA.

ANEXOS

ANEXO A. Árbol de Problemas



ANEXO B. 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 (incluido con resolución No JB-2005-834 de 20 de octubre del 2005)

LIBRO I.- NORMAS GENERALES PARA LAS INSTITUCIONES DEL

SISTEMA FINANCIERO

TITULO X.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS

CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO (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 la información y eventos externos; (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

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, toma de decisiones, ejecución de una transacción o entrega de un servicio; (reformado con resolución No. JB-2012-2148 de 26 de abril del 2012)

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 la 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; (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

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 la información; (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

2.18 Responsable de la información.- Es la persona encargada de cuidar la integridad, confidencialidad y disponibilidad de la información; debe tener autoridad para especificar y exigir las medidas de seguridad necesarias para cumplir con sus responsabilidades; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

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. Un plan de continuidad debe contener procedimientos que se ajusten a la realidad del negocio de cada institución; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

2.30 Administración de la continuidad.- Es un proceso permanente que garantiza la continuidad de las operaciones del negocio de las instituciones del sistema financiero, a través de la efectividad del mantenimiento del plan de continuidad; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

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

2.32 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;

2.33 Calidad de la información.- Es el resultado de la aplicación de los mecanismos implantados que garantizan la efectividad, eficiencia y confiabilidad de la información y los recursos relacionados con ella; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.34 Efectividad.- Es la garantía de que la información es relevante y pertinente y que su entrega es oportuna, correcta y consistente; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.35 Confiabilidad.- Es la garantía de que la información es la apropiada para la administración de la entidad, ejecución de transacciones y para el cumplimiento de sus obligaciones; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.36 Banca electrónica.- Son los servicios suministrados por las instituciones del sistema financiero a los clientes a través de internet en el sitio que corresponda a uno o más dominios de la institución, indistintamente del dispositivo tecnológico a través del cual se acceda; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.37 Banca móvil.- Son los servicios suministrados por las instituciones del sistema financiero a los clientes a través de equipos celulares mediante los protocolos propios de este tipo de dispositivos; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.38 Tarjetas.- Para efectos del presente capítulo, se refiere a las tarjetas de débito, de cajero automático y tarjetas de crédito; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.39 Canales electrónicos.- Se refiere a todas las vías o formas a través de las cuales los clientes o usuarios pueden efectuar transacciones con las instituciones del sistema financiero, mediante el uso de elementos o dispositivos electrónicos o tecnológicos, utilizando o no tarjetas. Principalmente son canales electrónicos: los cajeros automáticos (ATM), dispositivos de puntos de venta (POS y PIN Pad), sistemas de audio respuesta (IVR), señal telefónica, celular e internet u otro similares; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.40 Tarjeta inteligente.- Tarjeta que posee circuitos integrados (chip) que permiten la ejecución de cierta lógica programada, contiene memoria y microprocesadores y es capaz de proveer seguridad, principalmente en cuanto a la confidencialidad de la información de la memoria; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.41 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)

2.42 Transacción.- Se refiere a las acciones realizadas por los clientes a través de canales electrónicos, tales como: consultas, transferencias, depósitos, retiros, pagos, cambios de clave, actualización de datos y otras relacionadas; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

2.43 Incidente de tecnología de la información.- Evento asociado a posibles fallas en la tecnología de la información, fallas en los controles, o situaciones con probabilidad significativa de comprometer las operaciones del negocio; y, (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

2.44 Incidente de seguridad de la información.- Evento asociado a posibles fallas en la seguridad de la información, o una situación con probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

(incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

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 la información y por eventos externos. (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

El riesgo operativo incluye el riesgo legal en los términos establecidos en el numeral 2.41 del artículo 2. (inciso reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

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 la información.- Las instituciones controladas deben contar con la tecnología de la 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. (reformado con resolución No. JB-

2014-3066 de 2 de septiembre del 2014)

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir políticas, procesos, procedimientos y metodologías que aseguren una adecuada planificación y administración de la tecnología de la información. (inciso reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Dichas políticas, procesos, procedimientos y metodologías se referirán a: (inciso reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.1 Con el objeto de garantizar que la administración de la tecnología de la información soporte adecuadamente los requerimientos de operación actuales y futuros de la entidad, las instituciones controladas deben contar al menos con lo siguiente: (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.1.1 El apoyo y compromiso formal del directorio u organismo que haga sus veces y la alta gerencia, a través de la asignación de recursos

para el cumplimiento de los objetivos tecnológicos; (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.1.2 En función del tamaño y complejidad de las operaciones, las entidades deben conformar el comité de tecnología, que es el responsable de planificar, coordinar y supervisar las actividades de tecnología. El directorio asumirá las responsabilidades del comité de tecnología en las entidades que decidieran no conformarlo. La Superintendencia de Bancos y Seguros podrá disponer la conformación de este comité, si las condiciones de tamaño y complejidad de la entidad lo amerita. (numeral incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Dicho comité debe estará integrado como mínimo por: un delegado del directorio, quien lo presidirá, el representante legal de la institución y el funcionario responsable del área de tecnología;

4.3.1.3 Un plan funcional de tecnología de la información alineado con el plan estratégico institucional; y, un plan operativo que establezca las actividades a ejecutar en el corto plazo (un (1) año), traducido en tareas, cronogramas, personal responsable y presupuesto, de manera que se asegure el logro de los objetivos institucionales propuestos; (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.1.4 Tecnología de la información acorde a las operaciones del negocio y al volumen de transacciones, monitoreada y proyectada según las necesidades y crecimiento de la institución, con su correspondiente portafolio de proyectos tecnológicos a ejecutarse en el corto, mediano y largo plazo; (reformado con resolución No. JB-

2014-3066 de 2 de septiembre del 2014)

4.3.1.5 Políticas, procesos, procedimientos y metodologías de tecnología de la información definidos bajo estándares de general aceptación que garanticen la ejecución de los criterios de control interno de eficacia, eficiencia y cumplimiento, alineados a los objetivos y actividades de la institución, así como las consecuencias de la violación de éstas. (numeral sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Los procesos, procedimientos y metodologías de tecnología de la información deben ser revisados por el comité de tecnología y propuestos para la posterior aprobación del directorio o el organismo que haga sus veces;

4.3.1.6 Difusión y comunicación a todo el personal involucrado de las mencionadas políticas, procesos, procedimientos y metodologías, de tal forma que se asegure su implementación; y, (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.1.7 Una metodología de administración de proyectos que considere al menos su planificación, ejecución, control y cierre, enfocada en la optimización de recursos y la gestión de riesgos. (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.2 Con el objeto de garantizar que las operaciones de tecnología de la información satisfagan los requerimientos de la entidad, las instituciones controladas deben contar al menos con lo siguiente: (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.2.1 Procedimientos que establezcan las actividades y responsables de la operación y el uso de las instalaciones de procesamiento de información; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.2.2 Procedimientos de gestión de incidentes de tecnología de la información, que considere al menos su registro, priorización, análisis, escalamiento y solución; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.2.3 Inventario de la infraestructura tecnológica que considere por lo menos, su registro, responsables de uso y mantenimiento; y,

(incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.2.4 Procedimientos de respaldo de información periódicos, acorde a los requerimientos de continuidad del negocio que incluyan la frecuencia de verificación, las condiciones de preservación y eliminación y el transporte seguro hacia una ubicación remota, que no debe estar expuesto a los mismos riesgos del sitio principal.

(incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3 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:

4.3.3.1 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; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3.2 Un documento que refleje el alcance de los requerimientos funcionales; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3.3 Un documento que refleje los requerimientos técnicos y la relación y afectación a la capacidad de la infraestructura tecnológica actual;

(sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3.4 Ambientes aislados con la debida segregación de accesos, para desarrollo, pruebas y producción, los cuales deben contar con la capacidad requerida para cumplir sus objetivos. Al menos se debe contar con dos ambientes: desarrollo y producción; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3.5 Escaneo de vulnerabilidades en código fuente para identificar el nivel de riesgo del ambiente de la aplicación y en aplicaciones puestas en producción; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3.6 Pruebas técnicas y funcionales que reflejen la aceptación de los usuarios autorizados; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3.7 Procedimientos de control de cambios que considere su registro, manejo de versiones, segregación de funciones y autorizaciones e incluya los cambios emergentes; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3.8 Documentación técnica y de usuario permanentemente actualizada de las aplicaciones de la institución; y, (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3.9 Procedimientos de migración de la información, que incluyan controles para garantizar las características de integridad, disponibilidad y confidencialidad. (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.4 Con el objeto de garantizar que la infraestructura tecnológica que soporta las operaciones sea administrada, monitoreada y documentada, las instituciones controladas deben contar al menos con: (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.4.1 Procedimientos que permitan la administración, monitoreo y registros de configuración de las bases de datos, redes de datos, hardware y software base, que incluya límites y alertas; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.4.2 Un documento de análisis de la capacidad y desempeño de la infraestructura tecnológica que soporta las operaciones del negocio, que debe ser conocido y analizado por el comité de tecnología con una frecuencia mínima semestral. El documento debe incluir límites y alertas de al menos: almacenamiento, memoria, procesador, consumo de ancho de banda; y, para bases de datos: áreas temporales de trabajo, log de transacciones y almacenamiento de datos; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.4.3 Procedimientos de migración de la plataforma tecnológica, que incluyan controles para garantizar la continuidad del servicio; e,

(incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.4.4 Instalaciones de procesamiento de información crítica en áreas protegidas con los suficientes controles que eviten el acceso de personal no autorizado, daños a los equipos de computación y a la información en ellos procesada, almacenada o distribuida; y, condiciones físicas y ambientales necesarias para garantizar el correcto funcionamiento del entorno de la infraestructura de tecnología de la información. (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5 Medidas de seguridad en canales electrónicos.- Con el objeto de garantizar que las transacciones realizadas a través de canales electrónicos cuenten con los controles, medidas y elementos de seguridad para evitar el cometimiento de eventos fraudulentos y garantizar la seguridad y calidad de la información de los usuarios así como los bienes de los clientes a cargo de las instituciones controladas, éstas deberán cumplir como mínimo con lo siguiente: (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.1. Las instituciones del sistema financiero deberán adoptar e implementar los estándares y buenas prácticas internacionales de seguridad vigentes a nivel mundial para el uso y manejo de canales electrónicos y consumos con tarjetas, los cuales deben ser permanentemente monitoreados para asegurar su cumplimiento; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.2. Establecer procedimientos y mecanismos para monitorear de manera periódica la efectividad de los niveles de seguridad implementados en hardware, software, redes y comunicaciones, así como en cualquier otro elemento electrónico o tecnológico utilizado en los canales electrónicos, de tal manera que se garantice permanentemente la seguridad y calidad de la información; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.3. Canales de comunicación seguros mediante la utilización de técnicas de encriptación acorde con los estándares internacionales vigentes; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5.4. El envío de información de sus clientes relacionada con al menos números de cuentas y tarjetas, debe ser realizado bajo condiciones de seguridad de la información, considerando que cuando dicha información se envíe mediante correo electrónico o utilizando algún otro medio vía Internet, ésta deberá ser enmascarada; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5.5. La información confidencial que se transmita entre el canal electrónico y el sitio principal de procesamiento de la entidad, deberá estar en todo momento protegida mediante el uso de técnicas de encriptación acordes con los estándares internacionales vigentes y deberá evaluarse con regularidad la efectividad del mecanismo utilizado; (incluido con resolución No.

JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5.6. Las instituciones del sistema financiero deberán contar en todos sus canales electrónicos con software antimalware que esté permanentemente actualizado, el cual permita proteger el software instalado, detectar oportunamente cualquier intento o alteración en su código, configuración y/o funcionalidad, y emitir las alarmas correspondientes para el bloqueo del canal electrónico, su inactivación y revisión oportuna por parte de personal técnico autorizado de la institución; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.7. Las instituciones del sistema financiero deberán utilizar tecnología de propósito específico para la generación y validación de claves para ejecutar transacciones en los diferentes canales electrónicos y dicha información en todo momento debe estar encriptada; (incluido con

resolución No. JB2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB2014-3066 de 2 de septiembre del 2014)

4.3.5.8. Establecer procedimientos para monitorear, controlar y emitir alarmas en línea que informen oportunamente sobre el estado de los canales electrónicos, con el fin de identificar eventos inusuales, fraudulentos o corregir las fallas; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.9. Ofrecer a los clientes los mecanismos necesarios para que personalicen las condiciones bajo las cuales desean realizar sus transacciones que impliquen movimiento de dinero a través de los diferentes canales electrónicos y tarjetas, dentro de las condiciones o límites máximos que deberá establecer cada entidad. (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Entre las principales condiciones de personalización por cada tipo de canal electrónico, deberá constar: el registro de las cuentas a las cuales desea realizar transacciones monetarias, números de suministros de servicios básicos, números de telefonía fija y móvil, montos máximos por transacción diaria, semanal y mensual, entre otros. (sustituido con resolución No. JB-

2014-3066 de 2 de septiembre del 2014)

Para el caso de consumos con tarjetas, se deberán personalizar los cupos máximos, principalmente para los siguientes servicios: consumos nacionales, consumos en el exterior, compras por internet, entre otros; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.10. Requerir a los clientes que el registro y modificación de la información referente a su número de telefonía móvil y correo electrónico, se realicen por canales presenciales, además no se debe mostrar esta información por ningún canal electrónico;

(incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5.11. Las instituciones del sistema financiero deben registrar las direcciones IP y números de telefonía móvil desde las que se realizan las transacciones. Para permitir transacciones desde direcciones IP y telefonía móvil de otros países se debe tener la autorización expresa del cliente; (incluido con resolución No. JB-

2014-3066 de 2 de septiembre del 2014)

4.3.5.12. Incorporar en los procedimientos de administración de seguridad de la información la renovación de por lo menos una vez (1) al año de las claves de acceso a los canales electrónicos, la clave de banca electrónica debe ser diferente de aquella por la cual se accede a otros canales electrónicos; (incluido con resolución No.

JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5.13. Las instituciones deberán establecer procedimientos de control y mecanismos que permitan registrar el perfil de cada cliente sobre sus comportamientos transacciones que impliquen movimiento de dinero en el uso de canales electrónicos y tarjetas y definir procedimientos para monitorear en línea y permitir o rechazar de manera oportuna la ejecución de transacciones que impliquen movimiento de dinero que no correspondan a sus hábitos, lo cual deberá ser inmediatamente notificado al cliente mediante mensajería móvil, correo

electrónico, u otro mecanismo; (incluido con resolución No. JB-2012-

2148 de 26 de abril del 2012 y reformado con resolución No. JB-20143066 de 2 de septiembre del 2014)

4.3.5.14. Incorporar en los procedimientos de administración de la seguridad de la información, el bloqueo de los canales electrónicos o de las tarjetas cuando se presenten eventos inusuales que adviertan situaciones fraudulentas o después de un número máximo de tres (3) intentos de acceso fallido. Además, se deberán establecer procedimientos que permitan la notificación en línea al cliente a través de mensajería móvil, correo electrónico u

otro mecanismo, así como su reactivación de manera segura; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.15. Asegurar que exista una adecuada segregación de funciones entre el personal que administra, opera, mantiene y en general accede a los dispositivos y sistemas usados en los diferentes canales electrónicos y tarjetas; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.16. Las entidades deberán establecer procedimientos y controles para la administración, transporte, instalación y mantenimiento de los elementos y dispositivos que permiten el uso de los canales electrónicos y de tarjetas; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.17. Las instituciones del sistema financiero deben mantener sincronizados todos los relojes de sus sistemas de información que estén involucrados con el uso de canales electrónicos;

(incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.18. Mantener como mínimo durante doce (12) meses el registro histórico de todas las transacciones que se realicen a través de los canales electrónicos, el cual deberá contener como mínimo: fecha, hora, monto, números de cuenta (origen y destino en caso de aplicarse), código de la institución del sistema financiero de origen y de destino, número de transacción, código del dispositivo: para operaciones por cajero automático: código del ATM, para transacciones por internet: la dirección IP, para transacciones a través de sistemas de audio respuesta - IVR y para transacciones de banca electrónica mediante dispositivos móviles: el número de teléfono con el que se hizo la conexión.

En caso de presentarse reclamos, la información deberá conservarse hasta que se agoten las instancias legales. Si dicha información constituye respaldo contable se aplicará lo previsto en el tercer inciso

del artículo 80 de la Ley General de Instituciones del Sistema Financiero; (incluido con resolución No.

JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5.19. Incorporar en los procedimientos de administración de la seguridad de la información, controles para impedir que funcionarios de la entidad que no estén debidamente autorizados tengan acceso a consultar información confidencial de los clientes en ambiente de producción. En el caso de información contenida en ambientes de desarrollo y pruebas, ésta deberá ser enmascarada o codificada. Todos estos procedimientos deberán estar debidamente documentados en los manuales respectivos.

Además, la entidad deberá mantener y monitorear un log de auditoría sobre las consultas realizadas por los funcionarios a la información confidencial de los clientes, la cual debe contener como mínimo: identificación del funcionario, sistema utilizado, identificación del equipo (IP), fecha, hora, e información consultada. Esta información deberá conservarse por lo menos por doce (12) meses; (incluido con resolución No. JB-2012-2148 de

26 de abril del 2012)

4.3.5.20. Las instituciones del sistema financiero deberán poner a disposición de sus clientes un acceso directo como parte de su centro de atención telefónica (call center) para el reporte de emergencias bancarias, el cual deberá funcionar las veinticuatro (24) horas al día, los siete (7) días de la semana; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.21. Mantener por lo menos durante seis (6) meses la grabación de las llamadas telefónicas realizadas por los clientes a los centros de atención telefónica (call center), específicamente cuando se consulten saldos, consumos o cupos disponibles; se realicen reclamos; se reporten emergencias bancarias; o, cuando se actualice

su información. De presentarse reclamos, esa información deberá conservarse hasta que se agoten las instancias legales; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.22. Las entidades deberán implementar los controles necesarios para que la información de claves ingresadas por los clientes mediante sistemas de audio respuesta IVR), estén sometidas a técnicas de encriptación acordes con los estándares internacionales vigentes; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.23. Las instituciones del sistema financiero deberán enviar a sus clientes mensajes en línea a través de mensajería móvil, correo electrónico u otro mecanismo, notificando el acceso y la ejecución de transacciones realizadas mediante cualquiera de

los canales electrónicos disponibles, o por medio de tarjetas;

(incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y sustituido con resolución No. JB-2014-3021 de 30 de julio del 2014)

4.3.5.24. Las tarjetas emitidas por las instituciones del sistema financiero que las ofrezcan deben ser tarjetas inteligentes, es decir, deben contar con microprocesador o chip; y, las entidades controladas deberán adoptar los estándares internacionales de seguridad y las mejores prácticas vigentes sobre su uso y manejo; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.25. Mantener permanentemente informados y capacitar a los clientes sobre los riesgos derivados del uso de canales electrónicos y de tarjetas; y, sobre las medidas de seguridad que se deben tener en cuenta al momento de efectuar transacciones a través de éstos; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.26. Informar y capacitar permanentemente a los clientes sobre los procedimientos para el bloqueo, inactivación, reactivación y cancelación de los canales electrónicos ofrecidos por la entidad;

(incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5.27. Es función de auditoría interna verificar oportunamente la efectividad de las medidas de seguridad que las instituciones del sistema financiero deben implementar en sus canales electrónicos; así también deberán informar sobre las medidas correctivas establecidas en los casos de reclamos de los usuarios financieros que involucren debilidades o violación de los niveles de seguridad; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.28. Implementar técnicas de seguridad de la información en los procesos de desarrollo de las aplicaciones que soportan los canales electrónicos, con base en directrices de codificación segura a fin de que en estos procesos se contemple la prevención de vulnerabilidades; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.29. En todo momento en donde se solicite el ingreso de una clave, ésta debe aparecer enmascarada; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.6. Cajeros automáticos.- Con el objeto de garantizar la seguridad en las transacciones realizadas a través de los cajeros automáticos, las instituciones del sistema financiero deberán cumplir con las disposiciones del artículo 40, del capítulo I "Apertura y cierre de oficinas en el país y en el exterior, de las instituciones financieras privadas y públicas sometidas al control de la Superintendencia de Bancos y Seguros", del título II "De la organización de las instituciones del sistema financiero privado", de este libro y con lo siguiente: (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2013-2642 de 26 de septiembre del 2013)

4.3.6.1. Los dispositivos utilizados en los cajeros automáticos para la autenticación del cliente o usuario, deben encriptar la información ingresada a través de ellos; y, la información de las claves no debe ser almacenada en ningún momento; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.6.2. La institución controlada debe implementar mecanismos internos de autenticación del cajero automático que permitan asegurar que es un dispositivo autorizado por la institución del sistema financiero a la que pertenece; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.6.3. Los cajeros automáticos deben ser capaces de procesar la información de tarjetas inteligentes o con chip; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 l)

4.3.6.4. Los cajeros automáticos deben estar instalados de acuerdo con las especificaciones del fabricante, así como con los estándares de seguridad definidos en las políticas de la institución del sistema financiero, incluyendo el cambio de las contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.6.5. Establecer y ejecutar procedimientos de auditoría de seguridad en sus cajeros automáticos por lo menos una (1) vez al año, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que se brindan a través de estos. Los procedimientos de auditoría deberán ser ejecutados por personal capacitado y con experiencia; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2013-2642 de 26 de septiembre del 2013)

4.3.6.6. Para la ejecución de transacciones de clientes, se deberán implementar mecanismos de autenticación que contemplen por lo menos dos de tres factores: "algo que se sabe, algo que se tiene, o algo que se es"; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2013-2642 de 26 de septiembre del 2013)

4.3.6.7. Llevar a cabo campañas educativas para los usuarios acerca del uso, ubicación y medidas de seguridad pertinentes durante el uso del cajero, incluyendo la colocación de letreros alusivos a éstas en los recintos de los cajeros. (incluido con resolución No. JB-

2013-2642 de 26 de septiembre del 2013 l)

4.3.7. Puntos de venta (POS y PIN Pad).- Con el objeto de garantizar la seguridad en las transacciones realizadas a través de los dispositivos de puntos de venta, las instituciones del sistema financiero deberán cumplir como mínimo con lo siguiente: (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.7.1 Establecer procedimientos que exijan que los técnicos que efectúan la instalación, mantenimiento o desinstalación de los puntos de venta (POS y PIN Pad) en los establecimientos comerciales confirmen su identidad a fin de asegurar que este personal cuenta

con la debida autorización; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.7.2 A fin de permitir que los establecimientos comerciales procesen en presencia del cliente o usuario las transacciones efectuadas a través de los dispositivos de puntos de venta (POS o PIN Pad), éstos deben permitir establecer sus comunicaciones de forma inalámbrica segura; y, (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.7.3 Los dispositivos de puntos de venta (POS o PIN Pad) deben ser capaces de procesar la información de tarjetas inteligentes o con chip; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.8. Banca electrónica.- Con el objeto de garantizar la seguridad en las transacciones realizadas mediante la banca electrónica, las instituciones del sistema financiero que ofrezcan servicios por medio de este canal electrónico deberán cumplir como mínimo con lo siguiente: (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.8.1 Implementar los algoritmos y protocolos seguros, así como certificados digitales, que ofrezcan las máximas seguridades en vigor dentro de las páginas web de las entidades controladas, a fin de garantizar una comunicación segura, la cual debe incluir el uso de técnicas de encriptación de los datos transmitidos acordes con los estándares

internacionales vigentes; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.8.2 Realizar como mínimo una vez (1) al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación utilizados en la ejecución de transacciones por banca electrónica; y, en caso de que se realicen cambios en la plataforma que podrían afectar a la seguridad de este canal, se deberá efectuar una prueba adicional.

Las pruebas de vulnerabilidad y penetración deberán ser efectuadas por personal independiente a la entidad, de comprobada competencia y aplicando estándares vigentes y reconocidos a nivel internacional. Las instituciones deberán definir y ejecutar planes de acción sobre las vulnerabilidades detectadas;

(incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.8.3 Los informes de las pruebas de vulnerabilidad deberán estar a disposición de la Superintendencia de Bancos y Seguros, incluyendo un análisis comparativo del informe actual respecto del inmediatamente anterior; (incluido con resolución No. JB-2012-2148 de

26 de abril del 2012)

4.3.8.4 Implementar mecanismos de control, autenticación mutua y monitoreo, que reduzcan la posibilidad de que los clientes accedan a páginas web falsas similares a las propias de las instituciones del sistema financiero; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.8.5 Implementar mecanismos de seguridad incluyendo dispositivos tales como IDS, IPS, firewalls, entre otros, que reduzcan la posibilidad de que la información de las transacciones de los clientes sea capturada por terceros no autorizados durante la sesión; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.8.6 Establecer un tiempo máximo de inactividad, después del cual deberá ser cancelada la sesión y exigir un nuevo proceso de autenticación al

cliente para realizar otras transacciones; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.8.7 Se deberá informar al cliente al inicio de cada sesión, la fecha y hora del último ingreso al canal de banca electrónica; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.8.8 La institución del sistema financiero deberá implementar mecanismos para detectar la copia de los diferentes componentes de su sitio web, verificar constantemente que no sean modificados sus enlaces (links), suplantados sus certificados digitales, ni modificada indebidamente la resolución de su sistema de nombres de dominio (DNS); (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.8.9 La institución del sistema financiero debe implementar mecanismos de autenticación al inicio de sesión de los clientes, en donde el nombre de usuario debe ser distinto al número de cédula de identidad y éste así como su clave de acceso deben combinar caracteres numéricos y alfanuméricos con una longitud mínima de seis (6) caracteres; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.8.10 Para la ejecución de transacciones de clientes, se deberán implementar mecanismos de autenticación que contemplen por lo menos dos de tres factores: "algo que se sabe, algo que se tiene, o algo que se es", considerando que uno de ellos debe: ser dinámico por cada vez que se efectúa una transacción, ser una clave de una sola vez OTP (one time password), tener controles biométricos, entre otros; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.8.11 Para establecer las condiciones personales bajo las cuales los clientes realizarán sus transacciones por internet, tales como: matriculación de cuentas, definición de montos máximos, registro de números de teléfono celular, entre otros, que han sido definidos por la institución del sistema financiero, se debe validar o verificar la autenticidad del cliente a través de un canal diferente al de internet; (incluido con resolución

No. JB-2014-3021 de 30 de julio del 2014 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.9. Banca móvil.- Las instituciones del sistema financiero que presten servicios a través de banca móvil deberán sujetarse en lo que corresponda a las medidas de seguridad dispuestas en los subnumerales 4.3.5 y 4.3.8; (incluido

con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.10. Sistemas de audio respuestas (IVR).- Las instituciones del sistema financiero que presten servicios a través de IVR deberán sujetarse en lo que corresponda a las medidas de seguridad dispuestas en los subnumerales

4.3.5 y 4.3.8; y, (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.11. Corresponsales no bancarios.- Las instituciones financieras controladas que presten servicios a través de corresponsales no bancarios deberán sujetarse en lo que corresponda a las medidas de seguridad dispuestas en los subnumerales 4.3.5, 4.3.7 y 4.3.8. (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

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.

El directorio u organismo que haga sus veces de las instituciones del sistema financiero aprobará las políticas, normas, principios y procesos básicos de seguridad y protección para sus empleados, usuarios, clientes, establecimientos, bienes y patrimonio, así como para el resguardo en el transporte de efectivo y valores. (incluido con resolución No. JB-2011-1851 de 11 de enero del 2011)

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 la información adecuada. (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

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 la información y los eventos externos.

(reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

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 la información; y, (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

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 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 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 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 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 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.

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 administrar la continuidad del negocio, manteniendo procedimientos actualizados, a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción del negocio.

(artículo sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Para el efecto, las instituciones del sistema financiero deben establecer un proceso de administración de la continuidad del negocio, tomando como referencia el estándar ISO 22301 o el que lo sustituya, y considerar al menos lo siguiente:

15.1 La definición de objetivos, políticas, estrategias, procedimientos, metodología, planes y presupuesto para la administración de la continuidad;

15.2 Un comité de continuidad del negocio que esté conformado como mínimo por los siguientes miembros: el funcionario responsable de la unidad de riesgos, quien lo preside, el funcionario responsable de la administración de la continuidad, quien hará las veces de secretario, el funcionario responsable del área de tecnología de la información, el funcionario responsable del área de talento humano, el auditor interno, solo con voz, y el máximo representante de cada una de las áreas involucradas en el proceso de administración de la continuidad.

El comité de continuidad del negocio debe sesionar mínimo con la mitad más uno de sus integrantes, al menos una vez cada trimestre, y sus decisiones serán tomadas por mayoría absoluta de votos. El presidente del comité tendrá voto dirimente. El comité de continuidad del negocio debe dejar evidencia de las decisiones adoptadas, las cuales deben ser conocidas y aprobadas por el comité de administración integral de riesgos.

El comité de continuidad del negocio debe tener al menos las siguientes responsabilidades:

15.2.1. Monitorear la implementación del plan y asegurar el alineamiento de éste con la metodología; y, velar por una administración de la continuidad del negocio competente;

15.2.2. Proponer cambios, actualizaciones y mejoras al plan;

15.2.3. Revisar el presupuesto del plan y ponerlo en conocimiento del comité de administración integral de riesgos;

15.2.4. Dar seguimiento a las potenciales amenazas que pudieran derivar en una interrupción de la continuidad de las operaciones y coordinar las acciones preventivas; y,

15.2.5. Realizar un seguimiento a las medidas adoptadas en caso de presentarse una interrupción de la continuidad de las operaciones;

15.3 Análisis de impacto que tendría una interrupción de los procesos que soportan los principales productos y servicios. Para ello, deben determinar el impacto en términos de magnitud de daños, el período de recuperación y tiempos máximos de interrupción que puedan ocasionar los siniestros.

El análisis de impacto debe ser revisado periódicamente y actualizado cuando existan cambios en la organización o en su entorno, que puedan afectar sus resultados;

15.4 Análisis que identifique los principales escenarios de riesgos, incluyendo las fallas en la tecnología de la información, tomando en cuenta el impacto y la probabilidad de que sucedan. Para ello, debe seguirse una metodología consistente con aquella utilizada para la evaluación de los demás riesgos;

15.5 Evaluación y selección de estrategias de continuidad por proceso que permitan mantener la continuidad de los procesos que soportan los principales productos y servicios, dentro del tiempo objetivo de recuperación definido para cada proceso, mismas que deben tomar en cuenta, al menos lo siguiente: la seguridad del personal, habilidades y conocimientos asociados al proceso, instalaciones alternas

de trabajo, infraestructura alterna de procesamiento e información que soporte el proceso, seguridad de la información y equipamiento necesario para el proceso;

15.6 Realización de pruebas del plan de continuidad del negocio que permitan comprobar su efectividad y realizar los ajustes necesarios, cuando existan cambios que afecten la aplicabilidad del plan o al menos una (1) vez al año;

15.7 Procedimientos de difusión, comunicación, entrenamiento y concienciación del plan y su cumplimiento; e,

15.8 Incorporación del proceso de administración de la continuidad del negocio al proceso de administración integral de riesgos, que garantice la actualización y mejora continúa del plan de continuidad del negocio.

ARTÍCULO 16.- El plan de continuidad del negocio debe contener al menos los procedimientos operativos, tecnológicos, de emergencias y comunicaciones para cada proceso crítico y para cada escenario cubierto, los cuales deben considerar, según corresponda, como mínimo lo siguiente. (artículo sustituido con resolución No. JB-2014-3066 de

2 de septiembre del 2014)

16.1 Escenarios de riesgos y procesos críticos cubiertos y alertas de los escenarios y procesos críticos no cubiertos por el plan;

16.2 Roles y responsabilidades de las personas encargadas de ejecutar cada actividad;

16.3 Criterios de invocación y activación del plan;

16.4 Responsable de su actualización;

16.5 Acciones y procedimientos a ejecutar antes, durante y después de ocurrido el incidente que ponga en peligro la operatividad de la institución, priorizando la seguridad del personal;

16.6 Tiempos máximos de interrupción y de recuperación de cada proceso;

16.7 Acciones y procedimientos a realizar para trasladar las actividades de la institución a ubicaciones transitorias alternativas o para el restablecimiento de los procesos críticos de manera urgente;

16.8 Información vital y cómo acceder a ella (incluye información de clientes, contratos, pólizas de seguro, manuales técnicos y de operación, entre otros);

16.9 Comunicaciones con el personal involucrado, sus familiares y contactos de emergencia, para lo cual debe contar con la información para contactarlos oportunamente (direcciones, teléfonos, correos electrónicos, entre otros);

16.10 Interacción con los medios de comunicación;

16.11 Comunicación con los grupos de interés;

16.12 Establecimiento de un centro de comando (considerar al menos un sitio principal, y uno alterno); y,

16.13 Ante eventos de desastre en el centro principal de procesamiento, los procedimientos de restauración en una ubicación remota de los servicios de tecnología de la información deben estar dentro de los parámetros establecidos en el plan, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia. La ubicación remota no debe estar expuesta a los mismos riesgos del sitio principal.

SECCIÓN V.- RESPONSABILIDADES EN LA ADMINISTRACIÓN DEL RIESGO OPERATIVO

ARTÍCULO 17.- Las responsabilidades del directorio, 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", de este título. (artículo sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Adicionalmente, el directorio 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 políticas y estrategias relacionadas con la administración y gestión del riesgo operativo que permitan el cumplimiento de las disposiciones establecidas en este capítulo;

17.3 Podrá delegar la aprobación de los procesos, procedimientos y metodologías para la gestión de procesos, personas, tecnología de la información y servicios provistos por terceros a la instancia que considere pertinente, la misma que debe velar que los mismos estén alineados al cumplimiento de las políticas y estrategias de la administración del riesgo operativo aprobadas por el directorio; y,

17.4 Aprobar el proceso, metodología y plan para la administración de la continuidad del negocio.

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 de riesgos", del capítulo I "De la gestión integral y control de riesgos". (artículo sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Adicionalmente, el comité de administración integral de riesgos tendrá las siguientes responsabilidades en relación con la administración del riesgo operativo:

18.1 Evaluar y proponer para la aprobación del directorio las políticas para la administración del riesgo operativo;

18.2 Evaluar y proponer mejoras al proceso de administración de 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;

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

18.4 Evaluar y someter a aprobación del directorio el proceso, metodología y plan de continuidad del negocio a los que se refiere la sección IV, del este capítulo; asegurar su aplicabilidad; y, cumplimiento del mismo; y,

18.5 Analizar y aprobar la designación de líderes encargados de llevar a cabo las actividades previstas en el plan 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".

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 la información y los eventos externos;

(reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

19.3 Analizar las políticas y procedimientos propuestos por el área respectiva, para los procesos, personas, eventos externos y tecnología de la información, especialmente aquellas relacionadas con la seguridad de la información; (sustituido con resolución No. JB-2008-1202 de 23 de octubre del 2008 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

19.4 Liderar el desarrollo, la aplicabilidad y cumplimiento del proceso y plan de continuidad del negocio, al que se refiere la sección IV de este capítulo; así como proponer el nombre de los líderes de las áreas que deban cubrir el plan de continuidad del negocio, para lo cual debe designar de manera formal, un responsable del proceso de la administración de la continuidad, el cual debe tener a su cargo, entre otras, las siguientes funciones:

(reformado con resolución No. JB-20081202 de 23 de octubre del 2008 y sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

19.4.1 Proponer las políticas, procedimientos y metodologías para la administración de la continuidad del negocio, incluyendo la asignación de roles y responsabilidades;

19.4.2 Proponer cambios, actualizaciones y mejorar al plan de continuidad; e,

19.4.3 Informar al comité de continuidad los aspectos relevantes de la administración de la continuidad del negocio para una oportuna toma de decisiones; y,

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.- SERVICIOS PROVISTOS POR TERCEROS (incluida con resolución No. JB-2014-2798 de 19 de febrero del 2014)

ARTÍCULO 20.- Para mantener un adecuado control de los servicios provistos por terceros, incluidos las instituciones de servicios auxiliares del sistema financiero, las instituciones controladas deberán contar con un proceso integral para la administración de proveedores de servicios que incluya las actividades de pre contratación, suscripción, cumplimiento y renovación del contrato, para lo cual deberán por lo menos cumplir con lo siguiente:

(sustituido con resolución No. JB-2014-2798 de 19 de febrero del 2014)

20.1 Establecer políticas, procesos y procedimientos efectivos que aseguren una adecuada selección, calificación y evaluación de los proveedores, tales como:

20.1.1 Evaluación de la experiencia de la empresa o de su personal técnico en el mercado;

20.1.2 Desempeño de los proveedores en relación con los competidores;

20.1.3 Análisis de costo beneficio;

20.1.4 Evaluación financiera para asegurar la viabilidad del proveedor durante todo el período de suministro y cooperación previsto;

20.1.5 Análisis de informes de auditoría externa, si los tuviere;

20.1.6 Respuesta del proveedor a consultas, solicitudes de presupuesto y de ofertas;

20.1.7 Capacidad del servicio, instalación y apoyo e historial del desempeño en base a los requisitos;

20.1.8 Capacidad logística del proveedor incluyendo las instalaciones y recursos humanos;

20.1.9 La reputación comercial del proveedor en la sociedad así como de sus accionistas;

20.1.10 Identificación de proveedores de servicios críticos; y,

20.1.11 La exigencia de planes de contingencias del proveedor para los servicio a ser contratados;

20.2 Establecer políticas, procesos y procedimientos efectivos que aseguren una adecuada contratación de servicios, que garantice que los contratos incluyan como mínimo lo siguiente:

20.2.1 Niveles mínimos de calidad del servicio acordado;

20.2.2 Garantías técnicas y financieras, tales como: buen uso del anticipo, fiel cumplimiento del contrato, buen funcionamiento y disponibilidad del servicio, entre otros;

20.2.3 Multas y penalizaciones por incumplimiento;

20.2.4 Personal suficiente y calificado para brindar el servicio en los niveles acordados;

20.2.5 Transferencia del conocimiento del servicio contratado y entrega de toda la documentación que soporta el proceso o servicio;

20.2.6 La confidencialidad de la información y datos;

20.2.7 Derechos de propiedad intelectual del conocimiento, productos, datos e información, cuando aplique;

20.2.8 Definición del equipo de contraparte y administrador del contrato tanto de la institución del sistema financiero como del proveedor;

20.2.9 Definición detallada de los productos y servicios a ser entregados por el proveedor;

20.2.10 Cumplimiento por parte del proveedor de las políticas que establezca la institución del sistema financiero, las cuales deberán incluir al menos, la normativa expedida por la Superintendencia de Bancos y Seguros, aplicable en función del servicio a ser contratado; y,

20.2.11 Facilidades para la revisión y seguimiento del servicio prestado a las instituciones del sistema financiero, ya sea, por parte de la unidad de auditoría interna u otra área que la institución del sistema financiero designe, así como, por parte de los auditores externos.

20.3 Las instituciones del sistema financiero deberán aplicar metodologías para administrar los riesgos a los que se expone al contratar servicios provistos por terceros, particularmente de aquellos identificados como críticos;

20.4 Establecer políticas, procesos y procedimientos efectivos que aseguren un adecuado control y monitoreo de los servicios contratados, que incluyan como mínimo lo siguiente:

20.4.1 La evaluación, gestión y vigilancia de las actividades de prestación de los servicios contratados con terceros, a fin de garantizar que se cumplan en todo momento con los niveles mínimos de servicio acordados; y,

20.4.2 El monitoreo de los riesgos inherentes, particularmente del riesgo operacional y legal respecto del funcionamiento de aquellos servicios provistos por terceros, para lo cual deberán mantener una matriz de riesgos y evidencias de la gestión de los mismos; (reformado con resolución No. JB-

2014-3066 de 2 de septiembre del 2014)

20.5 Contar con proveedores alternos de los servicios críticos calificados bajo las disposiciones de esta normativa, que tengan la capacidad de prestar el servicio para mitigar el riesgo de dependencia en un sólo proveedor; y, (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

20.6 Si las instituciones del sistema financiero desean contratar la ejecución de los procesos productivos y/o servicios críticos en el exterior, deben notificar a la Superintendencia de Bancos y Seguros, adjuntando la documentación de respaldo que asegure el cumplimiento de este artículo. Además, las instituciones deben exigir al proveedor del servicio en el exterior, se encuentre sujeto a una supervisión efectiva por parte de la autoridad supervisora del país en el cual se brindará dicho servicio; y, que los servicios objeto de contratación en el exterior sean sometidos anualmente a un examen de auditoría independiente, por una empresa auditora de prestigio. (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Para cumplir con lo establecido en este capítulo, se deberá observar las disposiciones relativas a conflicto de intereses contenidas en el capítulo VIII "Principios de un buen gobierno corporativo", del título XIV "Código de transparencia y de derechos del usuario; y, en el capítulo IX "Principios de un buen gobierno corporativo para las instituciones financieras públicas", del título XXIII "De las disposiciones especiales para las instituciones financieras publicas", de este libro.

SECCIÓN VII.- SEGURIDAD DE LA INFORMACIÓN (incluida con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

ARTÍCULO 21.- Con el objeto de gestionar la seguridad de la información para satisfacer las necesidades de la entidad y salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas, las instituciones controladas deben tener como referencia la serie de estándares ISO/IEC 27000 o la que la sustituya y deben al menos: (artículo incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

21.1 Determinar funciones y responsables de la implementación y administración de un sistema de gestión de seguridad de la información que cumpla con los criterios de confidencialidad, integridad y disponibilidad, acorde al tamaño y complejidad de los

procesos administrados por el negocio; para lo cual las instituciones del sistema financiero podrán conformar un comité de seguridad de la información que se encargue de planificar, coordinar y supervisar el sistema de gestión de seguridad de la información.

El comité debe estar conformado como mínimo por: el miembro del directorio delegado al comité integral de riesgos, quien lo presidirá, el representante legal de la institución y el funcionario responsable de la seguridad de la información.

El organismo de control puede requerir la creación del comité y de una unidad especializada para la gestión de los sistemas de seguridad de la información en las instituciones del sistema financiero que por su complejidad y volumen de negocio lo requieran, así como en aquellas que no hubieren puesto en práctica de una manera adecuadas las disposiciones de este sección;

21.2 Establecer las políticas, procesos, procedimientos y metodologías de seguridad de la información definidos bajo estándares de general aceptación que garanticen la ejecución de los criterios de control interno de eficacia, eficiencia y cumplimiento, alineados a los objetivos y actividades de la institución, así como las consecuencias de violación de éstas.

Los procesos, procedimientos y metodologías de seguridad de la información deben ser revisados por el comité de seguridad de la información y en caso de no tener dicho comité, por el comité de administración integral de riesgos; y,

21.3 Difundir las políticas de seguridad de la información y propiciar actividades de concienciación y entrenamiento en estos temas.

ARTÍCULO 22.- Las instituciones deben establecer, implementar, ejecutar, monitorear, mantener y documentar un sistema de gestión de seguridad de la información que considere al menos lo siguiente: (artículo incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

22.1 Disponer de un inventario de la información con la designación de sus propietarios, mismos que deben tener como mínimo las siguientes responsabilidades:

22.1.1 Clasificar la información en términos de su valor, requerimientos legales, sensibilidad y criticidad para la entidad, éste debe ser revisado periódicamente con la finalidad de mantenerlo actualizado;

22.1.2 Definir y revisar periódicamente las restricciones y clasificaciones de acceso tomando en cuenta las políticas de control de acceso aplicables;

22.1.3 Autorizar los cambios funcionales a las aplicaciones; y,

22.1.4 Monitorear el cumplimiento de los controles establecidos;

22.2 Identificar y documentar los requerimientos mínimos de seguridad para cada tipo de información, con base en una evaluación de los riesgos que enfrenta la institución, aplicando la metodología de gestión de riesgo operativo de la entidad; y, con los controles de seguridad de la información;

22.3 Establecer procedimientos de eliminación de la información crítica de la entidad, de manera segura y considerando los requerimientos legales y regulatorios;

22.4 Mantener segregación de funciones y responsabilidades para mitigar los riesgos de modificación no autorizada o no intencionada o un mal uso de los activos de la organización;

22.5 Definir los procedimientos de gestión de cambios en los sistemas de información, hardware y software base, elementos de comunicaciones, entre otros, que consideren su registro, manejo de versiones, segregación de funciones y autorizaciones, e incluyan los cambios emergentes;

22.6 Procedimientos de afectación directa a las bases de datos que permitan identificar los solicitantes, autorizadores, y motivo de la modificación a la información, así como el registro de pistas de auditoría que facilite la trazabilidad del cambio;

22.7 Determinar los sistemas de control y autenticación tales como: sistemas de detección de intrusos (IDS), sistemas de prevención intrusos (IPS), firewalls, firewall de aplicaciones web (WAF), entre otros, para evitar accesos no autorizados, inclusive de terceros y, ataques externos especialmente a la información crítica;

22.8 Gestionar la realización de las auditorías de seguridad de la infraestructura tecnológica con base en el perfil de riesgo de la institución, por lo menos una (1) vez al año, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que se brindan. Los procedimientos de auditoría deben ser ejecutados por personal independiente a la entidad, capacitado y con experiencia, aplicando estándares vigentes y reconocidos a nivel internacional; estas auditorías deben incluir al menos pruebas de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación. Las instituciones deben definir y ejecutar planes de acción sobre las vulnerabilidades detectadas;

22.9 Controles 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 malicioso;

22.10 Medidas para proteger la información contenida en: documentos, medios de almacenamiento u otros dispositivos externos e intercambio electrónico, contra: robo, utilización o divulgación no autorizada de información para fines contrarios a los intereses de la entidad, por parte de su personal o de terceros;

22.11 Un procedimiento para el control de accesos a la información que considere la concesión; administración de derechos y perfiles para el registro, eliminación y modificación de la información, que garanticen una adecuada segregación de funciones y reduzcan el riesgo de error o fraude; así como la revocación de usuarios;

22.12 Establecer un procedimiento para el monitoreo periódico de accesos, operaciones privilegiadas, intentos de accesos no autorizados, para asegurar que los usuarios solo estén realizando actividades para las cuales han sido autorizados;

22.13 Implementar procedimientos que permitan contar con pistas de auditoría a nivel de aplicativos y bases de datos que registren los cambios realizados a la información crítica de la entidad. Los administradores no deben tener permiso para borrar o desactivar las pistas de sus propias actividades

22.14 Aplicar técnicas de encriptación sobre la información crítica, confidencial o sensible;

22.15 Considerar en la definición de requerimientos para nuevos sistemas o

mantenimiento, aquellos relacionados con la seguridad de la información;

22.16 Establecer procedimientos de gestión de incidentes de seguridad de la información, en los que se considere al menos su registro, priorización, análisis, escalamiento y solución;

22.17 Definir y mantener un sistema de registros históricos que permitan verificar el cumplimiento de las políticas, procesos, procedimientos y controles definidos para gestionar la seguridad de la información; y,

22.18 Evaluar periódicamente el desempeño del sistema de gestión de la seguridad de la información, a fin de tomar acciones orientadas a mejorarlo."

SECCIÓN VIII.- DISPOSICIONES GENERALES

ARTÍCULO 23.- 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 24.- 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.

ARTÍCULO 25.- 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.

ARTICULO 26.- 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.

SECCIÓN IX.- DISPOSICIONES TRANSITORIAS

PRIMERA.- Las disposiciones reformadas de esta norma deberán cumplirse conforme al siguiente cronograma: (disposición transitoria sustituida con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

1. Hasta el 31 de diciembre del 2014, debe cumplirse con los numerales: 4.3.5.1, 4.3.5.2, 4.3.5.4, 4.3.5.5, 4.3.5.7, 4.3.5.9, 4.3.5.13, 4.3.5.23, 4.3.5.28, 4.3.5.29, 4.3.6.1, 4.3.6.6, 4.3.7.2, 4.3.8.10, 4.3.8.11; (reformado con resolución No. SB-2014-1201 de 30 de diciembre del 2014)

2. Hasta junio del 2015, debe cumplirse con los numerales: 4.3.6.3 y 4.3.7.3; y, (incluido con resolución No. SB-2014-1201 de 30 de diciembre del 2014)

3. Hasta el 31 de diciembre del 2015, debe cumplirse con los todos los numerales de los siguientes numerales: 4.3.1, 4.3.2, 4.3.3, 4.3.4; con los numerales: 4.3.5.3, 4.3.5.10, 4.3.5.11, 4.3.5.12, 4.3.5.24; con las disposiciones normativas reformadas y contenidas en los artículos: 15, 16, 17, 18, 19, 21 y 22.

SEGUNDA.- Las instituciones del sistema financiero para dar cumplimiento a las disposiciones de la sección VI, de este capítulo, tendrán un plazo de trescientos sesenta (360) días, a partir de la publicación de esta reforma en el Registro Oficial. (reformada con resolución No. JB-2008-1223 de 18 de diciembre del 2008 y sustituida con resolución No. JB-20091491 de 26 de octubre del 2009, resolución No. JB-2011-1983 de 26 de agosto del 2011, resolución No. JB-2012-2358 de 25 de octubre del 2012 y resolución No. JB-2014-2798 de 19 de febrero del 2014)

TERCERA.- Las instituciones del sistema financiero deben reportar el nivel de cumplimiento de las disposiciones referidas en la primera y segunda transitoria en las siguientes fechas: 31 de enero del 2015, 31 de julio del 2015 y 31 de diciembre del 2015. (incluida con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

CUARTA.- El Banco del Instituto Ecuatoriano de Seguridad Social - BIESS implementará las disposiciones del numeral 4.3 Tecnología de la información" del artículo 4, conforme al siguiente cronograma: (incluida con resolución No. JB-2014-3033 de 6 de agosto del 2014)

1. Las disposiciones relacionadas con los factores: procesos, administración del riesgo operativo, servicios provistos por terceros y los numerales de canales electrónicos: 4.3.8.2, 4.3.8.3, 4.3.8.4, 4.3.8.11, 4.3.8.12, 4.3.8.18, 4.3.11.2, deben ser implementados hasta diciembre de 2014;

2. Las disposiciones relacionadas con el factor personas y los numerales de canales electrónicos: 4.3.8.1, 4.3.8.25, 4.3.8.16, 4.3.8.15, 4.3.8.7, 4.3.8.6, 4.3.11.10, 4.3.11.3,

   4.3.11.9 y 4.3.11.11, deben ser implementados hasta junio de 2015; y,

3. Las disposiciones normativas relacionadas con el factor tecnología de la información, deben ser implementadas hasta el mes de diciembre de 2015.

Adicionalmente, las disposiciones relacionadas con la continuidad del negocio, deben ser implementadas hasta el mes de octubre de 2016.

El ente de control en cualquier momento puede realizar una supervisión in situ a fin de verificar el avance del cumplimiento de acuerdo al cronograma enviado por la entidad.

ANEXO No.1

IDENTIFICACIÓN DE EVENTOS, FALLAS O INSUFICIENCIAS Y FACTORES DEL RIESGO OPERATIVO

LINEAS DE NEGOCIO:

TIPOS DE EVENTOS	FALLAS O INSUFICIENCIAS	FACTORES DE RIESGO DE OPERATIVO	NUMERO DE VECES (FRECUENCIA)	EFECTO CUANTITATIVO PERDIDA PRODUCIDA
FRAUDE INTERNO				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Operaciones no reveladas adecuadamente	Mal diseño de proceso	Procesos		
Operaciones no registradas intencionalmente	Inadecuada selección de personal	Personas		
Inadecuada utilización de información confidencial	Ausencia de control en los perfiles de usuario	Tecnología de Información		
Apropiación indebida de activos	Inadecuada segregación de funciones	Personas		
Falsificación	Inexistencia de controles	Procesos		
Destrucción maliciosa de activos	Inadecuadas medidas de seguridad	Procesos		
Evasión de impuestos	Falta de ética	Personas		
Robo	Inadecuada segregación de funciones	Personas		
FRAUDE EXTERNO				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Robo	Falta de seguridades físicas	Procesos		
Emisión de cheques sin fondos	Inadecuada capacitación del Personal	Personas		
Perjuicios por intrusión o ataque de terceros	Falta de seguridades en la teconología de información para prevenir ataques de terceros	Tecnología de Información		
Falsificación	Falta de seguridades de la tecnología de información	Tecnología de Información		
PRACTICAS DE EMPLEO Y SEGURIDAD DEL AMBIENTE DE TRABAJO				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Reclamos por compensación e indemnización al personal	Inadecuada contratación del personal	Procesos		
Violación de las normas de salud o seguridad	Falta de difusión y comunicación de políticas	Personas		
Todo tipo de discriminación	Inadecuada política de administración de personal	Personas		
PRACTICAS RELACIONADAS CON CLIENTES, LOS PRODUCTOS Y EL NEGOCIO				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Mal manejo de la información confidencial de clientes	Falta de defininición de políticas y procedimientos	Procesos		
Prácticas contrarias a la competencia, prácticas inadecuadas de negociación	Falta de defininición de políticas	Personas		
Actividades no autorizadas	Incursión en nuevas actividades sin considerar riesgos	Procesos		
Abuso de información privilegiada a favor de la institución	Falta de ética	Personas		
DAÑOS A LOS ACTIVOS FÍSICOS PROVOCADOS POR				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Terrorismo	Faltes de planes de contingencia (debidamente probados)	Eventos externos		
Vandalismo	Faltes de planes de contingencia (debidamente probados)	Eventos externos		
Pérdidas por desastres naturales	Faltes de planes de contingencia (debidamente probados)	Eventos externos		
INTERRUPCIÓN DEL NEGOCIO Y FALLAS EN LOS SISTEMAS				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Fallas en el software	Deficiencia en el proceso de desarrollo y/o implantación	Tecnología de Información		
Fallas en el hadware	Falta de previsión de la capacidad de los recursos para el volumen de operaciones. Falta de mantenimiento preventivo de los servidores centrales	Tecnología de Información		
Problemas de telecomunicación	Caída en los enlaces de telecomunicaciones	Tecnología de Información		
Cortes en los servicios públicos	Falta de planes de contingencia	Eventos externos		
DEFICIENCIAS EN LA EJECUCIÓN DE PROCESOS, EN EL PROCESAMIENTO DE OPERACIONES Y EN LAS RELACIONES CON PROVEEDORES Y OTROS EXTERNOS				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Errores en el ingreso de los datos	Falta de controles de ingreso de datos en las aplicaciones	Tecnología de Información		
Falla en la administración de colaterales	Inadecuada segregación de funciones	Procesos		
Documentación legal incompleta	Falta de verificación del área legal	Procesos		
Acceso no aprobado a las cuentas de clientes	Proceso no definido	Procesos		
Disputa con los proveedores	Deficiencias en la contratación	Procesos		
Incumplimiento en la entrega de la información hacia terceros	Falta de controles en el proceso de envio de información	Procesos		

NOTAS:

1.- En el presente Anexo constan ejemplos de eventos agrupados por tipo, los cuales consideran los lineamientos establecidos por el Comité de Basilea

2.- Los eventos que se produjeren que no esté alineados a los tipos de eventos especificados en este Anexo, deberán constar bajo la denominación "información no alineada, concepto bajo el cual constarán únicamente por excepción.

3.- Frecuencia, se refiere al número de veces que se repite cada evento

ANEXO C. Metodología Evaluación Riesgo Operativo

EVALUACION ADMINISTRACION DE RIESGO OPERATIVO

APLICACIÓN DE NORMATIVA / CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO; TÍTULO X .- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, DEL LIBRO I.- NORMAS GENERALES PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO

SECCIÓN II.- FACTORES DEL RIESGO OPERATIVO			Calificación de Riesgo						Si la respuesta es "No Cumple", completar datos del proyecto					NORMATIVA EXIGIBLE	
			0	1	2	3	4			Inicio	Fin			Detallar los requerimientos normativos exigibles a considerar para la verificación que la entidad cumple con lo estipulado.	
4.1. PROCESOS															
		ACTIVIDAD REQUERIDA													
PROCESOS	4.1 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	¿Se tiene identificado los procesos gobernantes?		1				1					Inventario de Procesos	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;
		¿Se tiene identificado los procesos operativos?		1				1					Inventario de Procesos	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.

		¿Se tiene identificado los procesos de apoyo?		1				1					Inventario de Procesos	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.	
		¿Se cuenta con la identificaciòn de los Procesos Críticos?		1				1					Inventario de Procesos/ Matriz de Procesos Críticos	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.		
		Las políticas deben referirse por lo menos a:														
		Diseño claro de los procesos, los cuales deben ser adaptables y dinámicos		1				1					Manual de Administración Integral de Riesgos	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.		
		Descripción en secuencia lógica y ordenada de las actividades, tareas, y controles.		1				1								
		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;		1				1								

		Difusión y comunicación de los procesos buscando garantizar su total aplicación		1				1						
		Actualización y mejora continua a través del seguimiento permanente en su aplicación.		1				1						
		Existe una adecuada separaciòn de funciones que evita concentraciones de carácter imposible?		1				1					Manual de Funciones	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.
		Mantienen inventario de procesos que cuentan con la siguiente informaciòn:											Inventario de Procesos	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.
		Tipo de proceso		1				1						
		Nombre de procesos		1				1						
		Responasble		1				1						
		Productos y servicios que genere el proceso		1				1						
		Clientes internos y externos		1				1						
		Fecha de aprobación		1				1						
		Fecha de actualización		1				1						
		Identicar sí es proceso crìtico		1				1						
			0	**18**	**0**	**0**	**0**	**18**						

CALIFICACION DE RIESGO	**1,00**	**bajo**

calificación	riesgo
1	bajo
0	0
0	0
0	0
0	0

Nivel Riesgo	Rango Mínimo	Rango Máximo	Riesgo
Uno	0	1	bajo
Dos	1,01	1,75	medio bajo
Tres	1,76	2,5	medio
Cuatro	2,51	3,25	medio alto
Cinco	3,26	4	alto

EVALUACION ADMINISTRACION DE RIESGO OPERATIVO

APLICACIÓN DE NORMATIVA / CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO; TÍTULO X .- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, DEL LIBRO I.- NORMAS GENERALES PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO

SECCIÓN II.- FACTORES DEL RIESGO OPERATIVO			De acuerdo al segmento que pertenece, colocar "1" si cumple o "0" si no cumple.						Si la respuesta es "No Cumple", completar datos del proyecto					NORMATIVA EXIGIBLE
			n/a	cumple	satisfactorio	parcialmente	no cumple	total	Procentaje de Avance de implementación	Fecha proyecto		Area responsable	Referencia	
			0	1	2	3	4			Inicio	Fin			Detallar los requerimientos normativos exigibles a considerar para la verificación que la entidad cumple con lo estipulado.
4.2. PERSONAS														
		ACTIVIDAD REQUERIDA												
PERSONAS	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.	**Los procesos de incorporación comprenden:**												
		Planificación de necesidades		1				1					Manual de Gestión Talento Humano	4.2.1 Los procesos de incorporación.- Que comprenden la planificación de necesidades, el reclutamiento, la selección, la contratación e inducción de nuevo personal;
		Procedimientos de Reclutamiento		1				1						
		Procedimientos de Selección		1				1						
		Procedimientos de contratación		1				1						
		Procedimientos de Inducción		1				1						
		Los procesos de permanencia comprenden:												
		Creación de condiciones laborales idóneas		1				1					Manual de Gestión Talento Humano	4.2.2 Los procesos de permanencia.- Que cubren la creación de condiciones laborales idóneas; la promoción
		Promoción de actividades de capacitación y formación		1				1						

		Existencia de un sistema de evaluación de desempeño		1				1					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,
		Desarrollo de carrera		1				1					
		Rendición de cuentas		1				1					
		Incentivos que motiven la adhesión de valores y controles institucionales		1				1					
		Los procesos de desvinculación comprenden:											
		Planificación de salida de personal		1				1				Manual de Gestión Talento Humano	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.
		Preparación de aspectos jurídcos		1				1					
		Finalización de la relación laboral		1				1					
			0	**14**	**0**	**0**	**0**	**14**					

CALIFICACION DE RIESGO	**1,00**	**bajo**

calificacion	riesgo
1	bajo
0	0
0	0
0	0
0	0

Nivel Riesgo	Rango Mínimo	Rango Máximo	Riesgo
Uno	0	1,00	bajo
Dos	1,01	1,75	medio bajo
Tres	1,76	2,50	medio
Cuatro	2,51	3,25	medio alto
Cinco	3,26	4,00	alto

EVALUACION ADMINISTRACION DE RIESGO OPERATIVO

APLICACIÓN DE NORMATIVA / CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO; TÍTULO X .- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, DEL LIBRO I.- NORMAS GENERALES PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO

SECCIÓN II.- FACTORES DEL RIESGO OPERATIVO			De acuerdo al segmento que pertenece, colocar "1" si cumple o "0" si no cumple.						Si la respuesta es "No Cumple", completar datos del proyecto					NORMATIVA EXIGIBLE	
			n/a	cumple	satisfactorio	parcialmente	no cumple	total	Porcentaje de Avance de implementación	Fecha proyecto		Área responsable	Referencia		
			0	1	2	3	4			Inicio	Fin			Detallar los requerimientos normativos exigibles a considerar para la verificación que la entidad cumple con lo estipulado.	
4.3. TECNOLOGÍA DE INFORMACION															
		ACTIVIDAD REQUERIDA													
TECNOLOGÍA DE	4.3.1 Garantizar que la administración de la tecnología de la información soporte adecuadamente los requerimientos de operación actuales y futuros de la entidad.	**¿El Directorio u organismo que haga sus veces y la Alta Gerencia asigna recursos para el cumplimiento de los objetivos tecnológicos?.**		1				1					Certificación del Presupuesto Aprobado	4.3.1.1	El apoyo y compromiso formal del directorio u organismo que haga sus veces y la alta gerencia, a través de la asignación de recursos para el cumplimiento de los objetivos tecnológicos
		¿Cuenta la entidad con un Comité de Tecnología o quien haga sus veces?.		1				1					Reglamento del Comité	4.3.1.2	Conformar el comité de tecnología. El directorio asumirá las responsabilidades del comité de tecnología en las entidades que decidieran no conformarlo.

		¿Cuenta la entidad con un Plan Operativo, Plan Anual de Tecnología de la Información y Plan de Seguridad de la Información?.		1				1					Plan Anual de TI y SI	4.3.1.3	Plan anual de tecnología de la información y plan operativo que establezca las actividades a ejecutar, traducido en tareas, cronogramas, personal responsable y presupuesto, de manera que se asegure el logro de los objetivos institucionales propuestos;
		¿Cuenta la entidad con la Tecnología de la información necesaria para atender el volumen de operaciones y transacciones del negocio y al volumen de transacciones?.		1				1					Análisis de Capacidad Tecnológica	4.3.1.4	Tecnología de la información acorde a las operaciones del negocio y al volumen de transacciones, monitoreada y proyectada.
		¿Cuenta la entidad con manuales de políticas, procesos y metodologías de tecnología de la información definidos bajo estándares de general aceptación, revisados por el comité de tecnología y debidamente aprobados por el directorio o el organismo que haga sus veces?.		1				1					Manuales de Teconología, Actas de Revisión del Comité de TI y Actas de Aprobación	4.3.1.5	Políticas, procesos, procedimientos y metodologías de tecnología de la información definidos bajo estándares de general aceptación.. Los procesos, procedimientos y metodologías de tecnología de la información deben ser revisados por el comité de tecnología y propuestos para la posterior aprobación del directorio o el organismo que haga sus veces.
		¿La entidad tiene planes de difusión y comunicación sobre riesgo tecnológico (incluye sistema de seguridad de información).		1				1					Planes de difusión y Comunicación, informe de avance	4.3.1.6	Difusión y comunicación al personal involucrado: políticas, procesos, procedimientos y metodologías, de tal forma que se asegure su implementación

		¿Cuenta la entidad con una metodología de administración de proyectos enfocada en la optimización de recursos y la gestión de riesgos?.		1				1					Metodología de Proyectos	4.3.1.7	Metodología de administración de proyectos que considere al menos su planificación, ejecución, control y cierre, enfocada en la optimización de recursos y la gestión de riesgos.
	4.3.2. Garantizar que las operaciones de tecnología de la información satisfagan los requerimientos de la entidad.	**Acorde a los requerimientos de un Plan de Continuidad de Negocio y el Sistema de Gestión de Seguridad de la Información, el Manual de Tecnología de la Información contempla:**													
		a). Polìticas y procedimientos de uso de las instalaciones de procesamiento de información.		1				1					Manual de Tecnología de Información	4.3.2.1	Procedimientos - Uso de las instalaciones de procesamiento de informaciónque: establecer actividades y responsables de la operación.
		b). Polìticas y procedimientos de gestión de incidentes de tecnología de la información (considera al menos su registro, priorización, análisis, escalamiento y solución).		1				1						4.3.2.2	Procedimientos de gestión de incidentes de tecnología de la información (considera al menos su registro, priorización, análisis, escalamiento y solución).
		c). Procedimientos de Respaldo de Información.		1				1						4.3.2.4	Procedimientos de respaldo de información periódicos, acorde a los requerimientos de continuidad del negocio: incluye frecuencia de verificación, las condiciones de preservación y eliminación, transporte seguro hacia una ubicación remota, entre otros.
		d). Inventario de la infraestructura tecnológica: identificación de item, registro,		1				1						4.3.2.3	Inventario de la infraestructura tecnológica:

		responsables de uso y mantenimiento												identificación de item, registro, responsables de uso y mantenimiento
4.3.3. Garantizar que el proceso de adquisición, desarrollo, implementación y mantenimiento de las aplicaciones satisfagan los objetivos del negocio.		**La Institución cuenta al menos con:**												
		1. Metodología para administración y control del proceso de compra de software y del ciclo de vida de desarrollo y mantenimiento de aplicaciones.		1				1					Metodologìas	4.3.3.1	Metodología para administración y control del proceso de compra de software y del ciclo de vida de desarrollo y mantenimiento de aplicaciones.
		2. Plan Operativo de necesidades tecnológicas.		1				1					Plan Operativo	4.3.3.3	Documento que refleje los requerimientos técnicos y la relación y afectación a la capacidad de la infraestructura tecnológica actual.
		3. Ambientes aislados con la debida segregación de accesos: desarrollo, pruebas y producción.		1				1					Informe de Ambientes de Aplicaciones	4.3.3.4	Ambientes aislados con la debida segregación de accesos: desarrollo, pruebas y producción. Contar con ambientes de desarrollo y producción.
		4. Escaneo de vulnerabilidades en códigos fuente.		1				1					Procedimiento de Escaneo	4.3.3.5	Escaneo de vulnerabilidades en código fuente para identificar el nivel de riesgo del ambiente de la aplicación y en aplicaciones puestas en producción
		5. Pruebas técnicas y funcionales que reflejen la aceptación de los usuarios autorizados		1				1					Procedimiento de Pruebas	4.3.3.6	Pruebas técnicas y funcionales que reflejen la aceptación de los usuarios autorizados
		6. Procedimientos de control de cambios.		1				1					Procedimientos de Control de Cambios	4.3.3.7	Procedimientos de control de cambios: registro, manejo de versiones, segregación de funciones y autorizaciones e

															incluya los cambios emergentes
		7. Documentación técnica y manuales de usuario de las aplicaciònes de la institución: actualizada		1				1					Manuales Técnicos y de Usuarios de aplicaciones	4.3.3.8	Documentación técnica y de usuario permanentemente actualizada de las aplicaciones de la institución
		8. Procedimientos de migración de la información.		1				1					Procedimientos de migración	4.3.3.9	Procedimientos de migración de la información: controles para garantizar las características de integridad, disponibilidad y confidencialidad.
	4.3.4. Garantizar que la infraestructura tecnológica que soporta las operaciones sea administrada, monitoreada y documentada:	**La Institución mantiene una Infraestructura Tecnológica que cumple al menos con lo siguiente:**													
		1. Análisis de la capacidad y desempeño de la infraestructura tecnológica que soporta las operaciones del negocio: revisado, analizado y aprobado por el comité de tecnología con una frecuencia mínima semestral.		1				1					Acta del Comité de TI en que se aprobó el análisis	4.3.4.2	Un documento de análisis de la capacidad y desempeño de la infraestructura tecnológica que soporta las operaciones del negocio, que debe ser conocido y analizado por el comité de tecnología con una frecuencia mínima semestral. El documento debe incluir límites y alertas de al menos: almacenamiento, memoria, procesador, consumo de ancho de banda; y, para bases de datos: áreas temporales de trabajo, log de transacciones y almacenamiento de datos;

		2. Instalaciones de procesamiento de información crítica en áreas protegidas: controles de acceso, daños a equipos y a la información en ellos procesada, almacenada o distribuida; y, condiciones físicas y ambientales necesarias.		1				1					Informe de Infraestructura Tecnológica	4.3.4.4	Instalaciones de procesamiento de información crítica en áreas protegidas: controles de acceso, daños a equipos y a la información en ellos procesada, almacenada o distribuida; y, condiciones físicas y ambientales necesarias para garantizar el correcto funcionamiento del entorno de la infraestructura de tecnología de la información.
		Acorde a los requerimientos de un Plan de Continuidad de Negocio y el Sistema de Gestión de Seguridad de la Información, el Manual de Tecnología de la Información contempla:													
		1. Los procedimientos para administración, monitoreo y registros de configuración de las bases de datos, redes de datos, hardware y software base; incluye una parametrización o jerarquización sobre accesos, límites y alertas.		1				1					Manual de Tecnología de Información	4.3.4.1	Procedimientos que permitan la administración, monitoreo y registros de configuración de las bases de datos, redes de datos, hardware y software base, que incluya límites y alertas
		2. Procedimientos de migración de la plataforma tecnológica.		1				1						4.3.4.3	Procedimientos de migración de la plataforma tecnológica, que incluyan controles para garantizar la continuidad del servicio;
CANALES	4.3.5. Seguridad de la Información	**La Institución, en lo relacionado a Seguridad de la Información, cuenta al menos con lo siguiente:**													
		1. Canales de comunicación seguros mediante la utilización de técnicas de encriptación acorde con los estándares internacionales vigentes;		1				1					Manual de Políticas de Seguridad de Ia Información	4.3.5.3	Canales de comunicación seguros mediante la utilización de técnicas de encriptación acorde con los estándares

													internacionales vigentes;
		2. Registro y respaldo de las direcciones IP y números de telefonía móvil desde las que se realizan las transacciones.		1				1				4.3.5.11	Las instituciones del sistema financiero deben registrar las direcciones IP y números de telefonía móvil desde las que se realizan las transacciones. Para permitir transacciones desde direcciones IP y telefonía móvil de otros países sedebe tener la autorización expresa del cliente
		3. Tarjetas inteligentes emitidas (con microprocesador o chip) adoptan estándares internacionales de seguridad y mejores prácticas vigentes sobre su uso y manejo.		1				1				4.3.5.24	Las tarjetas emitidas por las instituciones del sistema financiero que las ofrezcan deben ser tarjetas inteligentes, es decir, deben contar con microprocesador o chip; y, las entidades controladas deberán adoptar los estándares internacionales de seguridad y las mejores prácticas vigentes sobre su uso y manejo
		4. Los cajeros automáticos permiten procesar información de tarjetas inteligentes o con chip		1				1				4.3.6.3	Los cajeros automáticos deben ser capaces de procesar la información de tarjetas inteligentes o con chip
		5. Los dispositivos de puntos de venta (POS o PIN Pad) procesan información de tarjetas inteligentes o con chip.		1				1				4.3.7.3	Los dispositivos de puntos de venta (POS o PIN Pad) deben ser capaces de procesar la información de tarjetas inteligentes o con chip;

		6. Un manual de Tecnología de la Información que contiene:													
		a). Procedimientos y mecanismos para monitorear, controlar y actualizar niveles de seguridad implementados en hardware, software, redes y comunicaciones, así como en cualquier otro elemento electrónico o tecnológico utilizado en los canales electrónicos, de tal manera que se garantice permanentemente la seguridad y calidad de la información.		1				1					Manual de Tecnología de Información	4.3.5.2	Establecer procedimientos y mecanismos para monitorear de manera periódica la efectividad de los niveles de seguridad implementados en hardware, software, redes y comunicaciones, así como en cualquier otro elemento electrónico o tecnológico utilizado en los canales electrónicos, de tal manera que se garantice permanentemente la seguridad y calidad de la información; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012) .
		b). Procedimientos para monitorear, controlar y emitir alarmas en línea que informen oportunamente sobre el estado de los canales electrónicos.		1				1						4.3.5.8	Establecer procedimientos para monitorear, controlar y emitir alarmas en línea que informen oportunamente sobre el estado de los canales electrónicos, con el fin de identificar eventos inusuales, fraudulentos o corregir las fallas; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012).
		c). Procedimiento para que clientes de la entidad registren y modifiquen su información personal.		1				1						4.3.5.10	Requerir a los clientes que el registro y modificación de la información referente a su número de telefonía móvil y correo

															electrónico, se realicen por canales presenciales, además no se debe mostrar esta información por ningún canal electrónico
		d). Polìticas y procedimientos de un sistema de seguridad de la información aplicados a canales electrónicos, cajeros automáticos y banca electrónica.		1				1					4.3.5.12	Incorporar en los procedimientos de administración de seguridad de la información la renovación de por lo menos una vez (1) al año de las claves de acceso a los canales electrónicos, la clave de banca electrónica debe ser diferente de aquella por la cual se accede a otros canales electrónicos
													4.3.5.28	Implementar técnicas de seguridad de la información en los procesos de desarrollo de las aplicaciones que soportan los canales electrónicos, con base en directrices de codificación segura a fin de que en estos procesos se contemple la prevención de vulnerabilidades; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012).
													4.3.6.5.	Establecer y ejecutar procedimientos de auditoría de seguridad en sus cajeros automáticos por lo menos una (1) vez al año, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los

																servicios que se brindan a través de estos. Los procedimientos de auditoría deberán ser ejecutados por personal capacitado y con experiencia; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2013-2642 de 26 de septiembre del 2013).
															4.3.8.2	Realizar como mínimo una vez (1) al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación utilizados en la ejecución de transacciones por banca electrónica; y, en caso de que se realicen cambios en la plataforma que podrían afectar a la seguridad de este canal, se deberá efectuar una prueba adicional. Las pruebas de vulnerabilidad y penetración deberán ser efectuadas por personal independiente a la entidad, de comprobada competencia y aplicando estándares vigentes y reconocidos a nivel internacional. Las instituciones deberán definir y ejecutar planes de acción

														sobre las vulnerabilidades detectadas; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012).
			0	**32**	**0**	**0**	**0**	**32**						

CALIFICACION DE RIESGO	1,00	bajo

calificacion	riesgo
1	bajo
0	0
0	0
0	0
0	0

Nivel Riesgo	Rango Mínimo	Rango Máximo	Riesgo
Uno	0	1,00	bajo
Dos	1,01	1,75	medio bajo
Tres	1,76	2,50	medio
Cuatro	2,51	3,25	medio alto
Cinco	3,26	4,00	alto

EVALUACION ADMINISTRACION DE RIESGO OPERATIVO

APLICACIÓN DE NORMATIVA / CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO; TÍTULO X .- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, DEL LIBRO I.- NORMAS GENERALES PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO

SECCIÓN VI.- SERVICIOS PROVISTOS POR TERCEROS			**De acuerdo al segmento que pertenece, colocar "1" si cumple o "0" si no cumple.**						**Si la respuesta es "No Cumple", completar datos del proyecto**					**NORMATIVA EXIGIBLE**	
			n/a	**cumple**	**satisfactorio**	**parcialmente**	**no cumple**	**total**	Procentaje de Avance de implementación	Fecha proyecto		Area responsable	Referencia		
			0	**1**	**2**	**3**	**4**			Inicio	Fin			Detallar los requerimientos normativos exigibles a considerar para la verificación que la entidad cumple con lo estipulado.	
SERVICIOS PROVISTOS POR	Proceso integral para la administración de proveedores de servicios.	**Para mantener una adecuada administración de proveedores, la institución cuenta con un manual de procesos que cumple con Políticas, procesos y procedimientos elaborados y aplicados para selección, calificación y evaluación de los proveedores:**							1. Políticas, procesos y procedimientos elaborados y aplicados para selección, calificación y evaluación de los proveedores: reputación comercial, experiencia, desempeño, evaluación financiera, revisión de informes de auditoría, capacidad de servicio, instalaciones, capacidad logística, recurso humano, entre otros					ARTÍCULO 20.- Para mantener un adecuado control de los servicios provistos por terceros, incluidos las instituciones de servicios auxiliares del sistema financiero, las instituciones controladas deberán contar con un proceso integral para la administración de proveedores de servicios que incluya las actividades de pre contratación, suscripción, cumplimiento y renovación del contrato, para lo cual deberán por lo menos cumplir con lo siguiente:	
		Evaluación de la experiencia de la empresa o de su personal técnico en el mercado.		1				1					Manual de Servicios Generales	20.1: 20.1.1 - 20.1.10	Establecer políticas, procesos y procedimientos efectivos que aseguren una adecuada selección, calificación y evaluación de los proveedores:
		Medición del desempeño de los proveedores en relación con los competidores		1				1							
		Análisis de costo beneficio		1				1							

		Evaluación financiera para asegurar la viabilidad del proveedor durante todo el período de suministro y cooperación previsto		1				1							
		Análisis de informes de auditoría externa, si los tuviere		1				1							
		Verificación de respuestas del proveedor a consultas, solicitudes de presupuesto y de ofertas		1				1							
		Analizar la capacidad del servicio, instalación y apoyo e historial del desempeño en base a los requisitos		1				1							
		Análisis de la Capacidad logística del proveedor incluyendo las instalaciones y recursos humanos		1				1							
		Análisis de la reputación comercial del proveedor en la sociedad así como de sus accionistas		1				1							
		Identificación de proveedores de servicios críticos		1				1							
		La exigencia de planes de contingencias del proveedor para los servicio a ser contratados		1				1							
		Políticas, procesos y procedimientos efectivos que aseguren una adecuada contratación de servicios: niveles mìnimos de calidad, multas y penalizaciones, garantías, personal calificado, transferencia de conocimiento, confidencialidad, entre otros.		1				1				Manual de Servicios Generales	20.2	Establecer políticas, procesos y procedimientos efectivos que aseguren una adecuada contratación de servicios, que garantice que los contratos incluyan como mínimo lo siguiente:	
		Aplicación de metodologías para administrar los riesgos del factor servicios provistos por terceros, particularmente de aquellos identificados como críticos.		1				1					20.3	Las instituciones del sistema financiero deberán aplicar metodologías para administrar los riesgos a los que se expone al contratar servicios provistos por terceros,	

														particularmente de aquellos identificados como críticos
		Políticas, procesos y procedimientos para el control y monitoreo de servicios contratados.		1				1					20.4	Establecer políticas, procesos y procedimientos efectivos que aseguren un adecuado control y monitoreo de los servicios contratados, que incluyan como mínimo lo siguiente:
		La evaluación, gestión y vigilancia de las actividades de prestación de los servicios contratados con terceros.		1				1					20.4.1	La evaluación, gestión y vigilancia de las actividades de prestación de los servicios contratados con terceros, a fin de garantizar que se cumplan en todo momento con los niveles mínimos de servicio acordados;
		Monitoreo de los riesgos inherentes, particularmente del riesgo operacional y legal respecto del funcionamiento de aquellos servicios provistos por terceros, para lo cual deberán mantener una matriz de riesgos y evidencias de la gestión de los mismos		1				1					20.4.2	El monitoreo de los riesgos inherentes, particularmente del riesgo operacional y legal respecto del funcionamiento de aquellos servicios provistos por terceros, para lo cual deberán mantener una matriz de riesgos y evidencias de la gestión de los mismos
		Contar con proveedores alternos de los servicios críticos calificados, que tengan la capacidad de prestar el servicio para mitigar el riesgo de dependencia en un sólo proveedor.		1				1					20.5	Contar con proveedores alternos de los servicios críticos calificados bajo las disposiciones de esta normativa, que tengan la capacidad de prestar el servicio para mitigar el riesgo de dependencia en un sólo proveedor

		Cumplimiento de procesos y documentación relacionada sobre contratación de servicios en el exterior: Notificación a la Superintendencia de Bancos, documentación de respaldo, proveedor calificado por ente regulador del paìs de procedencia, procesos revisados por auditoría externa, entre otros.		1				1						20.6	Si las instituciones del sistema financiero desean contratar la ejecución de los procesos productivos y/o servicios críticos en el exterior, deben notificar a la Superintendencia de Bancos y Seguros, adjuntando ladocumentación de respaldo que asegure el cumplimiento de este artículo. Además, las instituciones deben exigir al proveedor del servicio en el exterior, se encuentresujeto a una supervisión efectiva por parte de la autoridad supervisora del país en el cual se brindará dicho servicio; y, que los servicios objeto de contratación en el exterior sean sometidos anualmente a un examen de auditoría independiente, por una empresa auditora de prestigio.

EVENTOS TEXTERNOS	Considerar la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos al control	Se cuenta con planes de contigencia, Plan de Emergencias y Planes de continuidad del negocio.		1			1					Planes aprobados por el Consejo de Administración.	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.
			0	**19**	**0**	**0**	**0**	**19**						

CALIFICACION DE RIESGO	**1,00**	**bajo**

calificacion	riesgo
1	bajo
0	0
0	0
0	0
0	0

Nivel Riesgo	Rango Mínimo	Rango Máximo	Riesgo
Uno	0	1	bajo
Dos	1,01	1,75	medio bajo
Tres	1,76	2,5	medio
Cuatro	2,51	3,25	medio alto
Cinco	3,26	4	alto

EVALUACION ADMINISTRACION DE RIESGO OPERATIVO

APLICACIÓN DE NORMATIVA / CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO; TÍTULO X .- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, DEL LIBRO I.- NORMAS GENERALES PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO

SECCIÓN VII.- SEGURIDAD DE LA INFORMACIÓN			**De acuerdo al segmento que pertenece, colocar "1" si cumple o "0" si no cumple.**						**Si la respuesta es "No Cumple", completar datos del proyecto**					**NORMATIVA EXIGIBLE**	
			n/a	**cumple**	**satisfactorio**	**parcialmente**	**no cumple**	**total**	Procentaje de Avance de implementación	Fecha proyecto		Area responsable	Referencia		
			0	**1**	**2**	**3**	**4**			Inicio	Fin			Detallar los requerimientos normativos exigibles a considerar para la verificación que la entidad cumple con lo estipulado.	
SEGURIDAD DE LA INFORMACIÓN	DEFINICIÓN Y PLANIFICACIÓN DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN.	**Para lograr un Sistema de Gestión de Seguridad de la Información, la institución ha definido y planicado las siguientes fases:**												**ARTÍCULO 21.- Con el objeto de gestionar la seguridad de la información para satisfacer las necesidades de la entidad y salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas, las instituciones controladas deben tener como referencia la serie de estándares ISO/IEC 27000 o la que la sustituya y deben al menos:**	
		1. Contar con el compromiso de la Alta Gerencia para la implementación de un Sistema de Gestiòn de Seguridad de la Información.												21.1	Determinar funciones y responsables de la implementación y administración de un sistema de gestión de seguridad de la información que cumpla con los criterios de confidencialidad, integridad y disponibilidad, acorde al tamaño y complejidad de los procesos
		a) Definir funciones y responsables de la implementación y administración del sistema de gestión de seguridad de la información.		1				1					Manual de Funciones de la Unidad de SI o del Responsable		

		b) Reglamento del Comité de Seguridad de la Información aprobado por el Directorio o quien haga sus veces.		1				1				Reglamento del Comité correspondiente		administrados por el negocio; para lo cual las instituciones del sistema financiero podrán conformar un comité de seguridad de la información que se encargue de planificar, coordinar y supervisar el sistema de gestión de seguridad de la información. El comité debe estar conformado como mínimo por: el miembro del directorio delegado al comité integral de riesgos, quien lo presidirá, el representante legal de la institución y el funcionario responsable de la seguridad de la información. El organismo de control puede requerir la creación del comité y de una unidad especializada para la gestión de los sistemas de seguridad de la información en las instituciones del sistema financiero que por su complejidad y volumen de negocio lo requieran, así como en aquellas que no hubieren puesto en práctica de una manera adecuadas las disposiciones de este sección.
		c) Comitè de Seguridad de la Información conformado.		1				1				Detalle de Integrantes del Comité de SI o su equivalente		
		d) Funciones y responsabilidades definidas de la unidad especializada para la gestión de los sistemas de seguridad de la información.		1				1				Manual de Funciones de la Unidad de SI o del Responsable		
		2. Políticas, procesos, procedimientos y metodologías de seguridad de la información definidos bajo estándares de general aceptación y revisados por el comité de seguridad de la información y en conocimiento del comité AIR.		1				1				Manual de Polìticas de Seguridad de Información	21.2	Establecer las políticas, procesos, procedimientos y metodologías de seguridad de la información definidos bajo estándares de general aceptación que garanticen la ejecución de los criterios de control interno de eficacia, eficiencia y cumplimiento, alineados

																a los objetivos y actividades de la institución, así como las consecuencias de violación de éstas. Los procesos, procedimientos y metodologías de seguridad de la información deben ser revisados por el comité de seguridad de la información y en caso de no tener dicho comité, por el comité de administración integral de riesgos .
		3. Capacitación y difusión de políticas y plan seguridad de la información y, programa de concienciación y entrenamiento del plan.		1			1					Plan de Capacitación y Difusión e informe de cumplimiento	21.3	Difundir las políticas de seguridad de la información y propiciar actividades de concienciación y entrenamiento en estos temas.
	IMPLEMENTACIÓN, MANTENIMIENTO Y ACTUALIZACIÓN DEL PLAN DE GESTION DE SEGURIDAD DE LA INFORMACIÓN	**El Plan de Gestión de Seguridad de la Información considera al menos lo siguiente:**											**ARTÍCULO 22.- Las instituciones deben establecer, implementar, ejecutar, monitorear, mantener y documentar un sistema de gestión de seguridad de la información que considere al menos lo siguiente:**		
		1. Inventario de la información con la designación de sus propietarios											22.1	Disponer de un inventario de la información con la designación de sus propietarios, mismos que deben tener como mínimo las siguientes responsabilidades:
		a). Información clasificada en términos de su valor, requerimientos legales, sensibilidad y criticidad para la entidad. Revisado periódicamente con la finalidad de mantenerlo actualizado.		1			1					Inventario y clasificación de la Información	22.1.1	Clasificar la información en términos de su valor, requerimientos legales, sensibilidad y criticidad para la entidad, éste debe ser revisado periódicamente con la finalidad de mantenerlo actualizado
		b). Definición de polìticas, parámetros y claves de acceso y,		1			1					Políticas de Gestión de Seguridad de Información	22.1.2	Definir y revisar periódicamente las restricciones y clasificaciones de

		procedimiento de actualización.												acceso tomando en cuenta las políticas de control de acceso aplicables
		c). Polìticas y procedimientos de cambios funcionales a las aplicaciones.		1			1						22.1.3	Autorizar los cambios funcionales a las aplicaciones
		d). Plan de monitoreo de controles establecidos.		1			1					Plan de monitoreo	22.1.4	Monitorear el cumplimiento de los controles establecidos
		2. Documento con la evaluación, identificación y análisis de requerimientos mínimos de seguridad para cada tipo de información:		1			1					Análisis de Riesgos de la Información	22.2	Identificar y documentar los requerimientos mínimos de seguridad para cada tipo de información, con base en una evaluación de los riesgos que enfrenta la institución, aplicando la metodología de gestión deriesgo operativo de la entidad; y, con los controles de seguridad de la información
		3. Procedimientos de eliminación de la información crítica de la entidad, de manera segura y considerando los requerimientos legales y regulatorios		1			1					Procedimientos de eliminación de información crítica	22.3	Establecer procedimientos de eliminación de la información crítica de la entidad, de manera segura y considerando los requerimientos legales y regulatorios
		4. Segregación de funciones y responsabilidades para mitigar los riesgos de modificación no autorizada o no intencionada o un mal uso de los activos de la organización.		1			1					Procedimientos de Seguridad de la Información	22.4	Mantener segregación de funciones y responsabilidades para mitigar los riesgos de modificación no autorizada o no intencionada o un mal uso de los activos de la organización.
		5. Procedimientos de gestión de cambios en los sistemas de información, hardware y software base, elementos de comunicaciones, entre otros, que consideren su registro, manejo de versiones, segregación de funciones y autorizaciones, e incluyan los cambios emergentes.		1			1					Procedimientos de Gestón de Cambios	22.5	Definir los procedimientos de gestión de cambios en los sistemas de información, hardware y software base, elementos de comunicaciones, entre otros, que consideren su registro, manejo de versiones, segregación de funciones y autorizaciones, e

														incluyan los cambios emergentes.
		6. Procedimientos de afectación directa a las bases de datos que permitan identificar los solicitantes, autorizadores, y motivo de la modificación a la información, así como el registro de pistas de auditoría que facilite la trazabilidad del cambio.		1				1				Procedimientos de Afectaciòn a bases de datos	22.6	Procedimientos de afectación directa a las bases de datos que permitan identificar los solicitantes, autorizadores, y motivo de la modificación a la información, así como el registro de pistas de auditoría que facilite la trazabilidad del cambio.
		7. Sistemas de control y autenticación : sistemas de detección de intrusos (IDS), sistemas de prevención intrusos (IPS), firewalls, firewall de aplicaciones web (WAF), entre otros, para evitar accesos no autorizados, inclusive de terceros y, ataques externos especialmente a la información crítica.		1				1				Informe de Sistemas de control y autententicación implementados	22.7	Determinar los sistemas de control y autenticación tales como: sistemas de detección de intrusos (IDS), sistemas de prevención intrusos (IPS), firewalls, firewall de aplicaciones web (WAF), entre otros, para evitar accesos no autorizados, inclusive de terceros y, ataques externos especialmente a la información crítica
		8. Informes de procedimientos de auditorías de seguridad de la infraestructura tecnológica donde se evalúe los controles implementados en función de la identificación de riesgos (inherentes y residuales) de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación. Planes de acción sobre las vulnerabilidades detectadas con el fin de mitigar los riesgos que podrían afectar a la seguridad de los servicios que se brindan.		1				1				Informes de Auditorías de Seguridad de Información	22.8	Gestionar la realización de las auditorías de seguridad de la infraestructura tecnológica con base en el perfil de riesgo de la institución, por lo menos una (1) vez al año, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios quese brindan. Los procedimientos de auditoría deben ser ejecutados por personal independiente a la entidad, capacitado y con experiencia, aplicando estándares vigentes y reconocidos a nivel

														internacional; estas auditorías deben incluir al menos pruebas de vulnerabilidad y penetración a los equipos, dispositivos y medios decomunicación. Las instituciones deben definir y ejecutar planes de acción sobre lasvulnerabilidades detectadas
		9. Controles 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 malicioso		1				1				Informe de controles implementados	22.9	Controles para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia, así como instalar y actualizarperiódicamente aplicaciones de detección y desinfección de virus informáticos y demás software malicioso
		10. Planes y procedimientos implementados para proteger la información contenida en: documentos, medios de almacenamiento u otros dispositivos externos e intercambio electrónico, contra: robo, utilización o divulgación no autorizada de información para fines contrarios a los intereses de la entidad, por parte de su personal o de terceros.		1				1				Procedimientos para proteger la información	22.10	Medidas para proteger la información contenida en: documentos, medios de almacenamiento u otros dispositivos externos e intercambio electrónico, contra: robo, utilización o divulgación no autorizada de información para fines contrarios a los intereses de la entidad, por parte de su personal o de terceros
		11. Procedimiento para el control de accesos a la información que considere la concesión; administración de derechos y perfiles para el registro, eliminación y modificación de la información, que garanticen una adecuada segregación de funciones y reduzcan el riesgo de error o fraude; así como la revocación de usuarios.		1				1				Procedimientos para control de accesos a la información	22.11	Un procedimiento para el control de accesos a la información que considere la concesión; administración de derechos y perfiles para el registro, eliminación y modificación de la información, que garanticen una adecuada segregación de funciones y reduzcan el riesgo de error o fraude; así como la revocación de usuarios

		12. Procedimiento para el monitoreo periódico de accesos, operaciones privilegiadas e intentos de accesos no autorizados.		1				1				Procedimiento para el monitoreo de accesos	22.12	Establecer un procedimiento para el monitoreo periódico de accesos, operaciones privilegiadas, intentos de accesos no autorizados, para asegurar que los usuarios solo estén realizando actividades para las cuales han sido autorizados.
		13. Procedimientos que permitan contar con pistas de auditoría a nivel de aplicativos y bases de datos que registren los cambios realizados a la información crítica de la entidad. Los administradores no deben tener permiso para borrar o desactivar las pistas de sus propias actividades.		1				1				Procedimientos de Auditorìa de aplicativos y bases de datos	22.13	Implementar procedimientos que permitan contar con pistas de auditoría a nivel de aplicativos y bases de datos que registren los cambios realizados a la información crítica de la entidad. Los administradores no deben tener permiso para borrar o desactivar las pistas de sus propias actividades.
		14. Aplicación del procedimiento y técnicas de encriptación sobre la información crítica, confidencial o sensible.		1				1				Inventario de la Información crítica en la que se ha aplicado técnicas de encriptación	22.14	Aplicar técnicas de encriptación sobre la información crítica, confidencial o sensible.
		15. Plan de adquisición y mantenimiento de sistemas: requerimientos relacionados con la seguridad de la información.		1				1				Plan de adquisición y mantenimiento de sistemas de SI	22.15	Considerar en la definición de requerimientos para nuevos sistemas o mantenimiento, aquellos relacionados con la seguridad de la información.
		16. Procedimientos de gestión de incidentes de seguridad de la información, en los que se considere al menos su registro, priorización, análisis, escalamiento y solución		1				1				Procedimientos de Gestión de Incidentes de SI	22.16	Establecer procedimientos de gestión de incidentes de seguridad de la información, en los que se considere al menos su registro, priorización, análisis, escalamiento y solución

		17. Sistema de registros históricos que permitan verificar el cumplimiento de las políticas, procesos, procedimientos y controles definidos para gestionar la seguridad de la información		1			1					Informe de Auditoría Interna de la Seguridad de Información	22.17	Definir y mantener un sistema de registros históricos que permitan verificar el cumplimiento de las políticas, procesos, procedimientos y controles definidos para gestionar la seguridad de la información
		18. Evaluación anual del desempeño del sistema de gestión de la seguridad de la información: informes, acciones correctivas y mejoramiento.		1			1					Informe de Evaluación del desempeño del plan de gestión de la SI	22.18	Evaluar periódicamente el desempeño del sistema de gestión de la seguridad de la información, a fin de tomar acciones orientadas a mejorarlo.
			0	**27**	**0**	**0**	**0**	**27**						

CALIFICACION DE RIESGO	**1,00**	**bajo**

calificacion	riesgo
1	bajo
0	0
0	0
0	0
0	0

Nivel Riesgo	Rango Mínimo	Rango Máximo	Riesgo
Uno	0	1	bajo
Dos	1,01	1,75	medio bajo
Tres	1,76	2,5	medio
Cuatro	2,51	3,25	medio alto
Cinco	3,26	4	alto

EVALUACION ADMINISTRACION DE RIESGO OPERATIVO

APLICACIÓN DE NORMATIVA / CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO; TÍTULO X .- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, DEL LIBRO I.- NORMAS GENERALES PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO

		SECCIÓN III.- SECCIÓN III.- ADMINISTRACIÓN DEL RIESGO OPERATIVO	**De acuerdo al segmento que pertenece, colocar "1" si cumple o "0" si no cumple.**						**Si la respuesta es "No Cumple", completar datos del proyecto**					**NORMATIVA EXIGIBLE**
			n/a	**cumple**	**satisfactorio**	**parcialmente**	**no cumple**	**total**	Procentaje de Avance de implementación	Fecha proyecto		Area responsable	Referencia	Detallar los requerimientos normativos exigibles a considerar para la verificación que la entidad cumple con lo estipulado.
			0	**1**	**2**	**3**	**4**			Inicio	Fin			
ADMINISTRACION DE RIESGO	Procesos de Administraciòn de Riesgo Operativo	**¿Cuenta la institución con procesos de administración de Riesgo Operativo?.**		**1**				**1**					Manual Integral de Riesgos	Art 5. El diseño del proceso de administración de riesgo operativo deberápermitir 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.
		Para una adecuada administración del riesgo operativo la institucion cuenta con:												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
		Codigo de Etica y Conducta		1				**1**					Codigo de Etica y Reglamento Inerno	
		Cultura de Control Interno		1				**1**						

		Planes de Contigencia		1				**1**					Plan de Contigencia	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 la información adecuada. (reformado con resolución No. JB-2014-3066 de 2 de s eptiembre del 2014)
		Plan de Continuidad de Negocio		1				**1**					Plan de Continuidad Negocio	
		Tecnología de la Información adecuada		1				**1**					Plan de Contigencia TI	
	Lineas de Negocio	**Se cuenta con agrupación de los procesos por líneas de negocio de acuerdo a una metodología establecida de manera formal y por escrito**												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:
		¿La institución cuenta con procesos productivos que se asignan a las líneas de negocio de acuerdo con los productos y servicios que generan?		1				**1**					Inventario de Procesos	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;
		¿Las líneas de negocio agrupan los procesos gobernantes y los procesos habilitantes que intervienen en las mismas?		1				**1**					Inventario de Procesos	7.2as 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.
		¿Se identifica por línea de negocio, los eventos de riesgo operativo, agrupados por tipo de evento?		1				**1**					Inventario de Procesos	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 la información y los eventos

															externos. (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)
	Orden legal	**Se determina 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?**		1				**1**					Manual Integral de Riesgos / Metodología Orden Legal		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 se enfocar por lo menos a los siguientes campos:													
		Actos Societarios		1				**1**						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 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;
		Gestiòn de Crèdito		1				**1**						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;
		Operación del giro financiero		1				**1**					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;
		Actividades complementarias de las operaciones del giro financiero		1				**1**					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,
		Cumplimiento legal y normativo		1				**1**					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)

	Base de datos	**¿Se ha conformado bases de datos centralizadas, suficientes y de calidad, que permitan registrar, ordenar, clasificar y disponer de información sobre los eventos de riesgo operativo?**		1			**1**				Sistema de Administraciòn Riesgo Operativo	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 REPÚBLICA DEL ECUADOR SUPERINTENDENCIA DE BANCOS Y SEGUROS 647 pérdidas esperadas e inesperadas atribuibles a este riesgo. (artículo reformado con resolución No. JB-2008-1202 de 23 de octubre del 2008)
	Control Interno	**¿ Se cuenta con un sistema de Control Interno que permita generar respuestas oportunas ante diversos eentos de riesgo operativo?**		1			**1**				Sistema de Control Interno	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.

	Reportes Riesgo Operativo	**¿ Se cuenta con un esquema organizado de reportes que permitan gestionar el riesgo Operativo?**		1				**1**					Informes Area de Riesgos	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.	
		Los reportes contienen al menos lo siguiente:													
		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		**1**				**1**					Informes Area de Riesgos	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;
		Informes de evaluación del grado de cumplimiento de las políticas relacionadas con los factores de riesgo operativo, procesos y procedimientos establecidos por la institución.		**1**				**1**						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.
		Indicadores de gestión que permitan evaluar la eficiencia y eficacia de las políticas, procesos y procedimientos aplicados.		**1**				**1**						14.3	Indicadores de gestión que permitan evaluar la eficiencia y eficacia de las políticas, procesos y procedimientos aplicados.
			0	**21**	**0**	**0**	**0**	**21**							

CALIFICACION DE RIESGO	**1,00**	**bajo**

calificacion	riesgo
1	bajo
0	0
0	0
0	0
0	0

Nivel Riesgo	Rango Mínimo	Rango Máximo	Riesgo
Uno	0	1	bajo
Dos	1,01	1,75	medio bajo
Tres	1,76	2,5	medio
Cuatro	2,51	3,25	medio alto
Cinco	3,26	4	alto

EVALUACION ADMINISTRACION DE RIESGO OPERATIVO

APLICACIÓN DE NORMATIVA / CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO; TÍTULO X .- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, DEL LIBRO I.- NORMAS GENERALES PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO

SECCIÓN V.- RESPONSABILIDADES EN LA ADMINISTRACIÓN DEL RIESGO			**De acuerdo al segmento que pertenece, colocar "1" si cumple o "0" si no cumple.**						**Si la respuesta es "No Cumple", completar datos del proyecto**					**NORMATIVA EXIGIBLE**	
			n/a	**cumple**	**satisfactorio**	**parcialmente**	**no cumple**	**total**	Procentaje de Avance de implementación	Fecha proyecto		Area responsable	Referencia		
			0	**1**	**2**	**3**	**4**			Inicio	Fin			Detallar los requerimientos normativos exigibles a considerar para la verificación que la entidad cumple con lo estipulado.	
ADMINISTRACION DEL RIESGO OPERATIVO	Responsabilidades del Directorio.	**¿Las funciones y responsabilidades del Directorio respecto a la Administración del Riesgo Operativo contemplan al menos lo siguiente?**												**ARTÍCULO 17.- Las responsabilidades del directorio, 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", de este título. Adicionalmente, el directorio tendrá las siguientes responsabilidades en relación con la administración del riesgo operativo:**	
		1. Crear una cultura organizacional con principios y valores de comportamiento ético. Políticas y estrategias definidas y relacionadas con la administración y gestión del riesgo operativo.		1				1					Reglamento o Manual de funciones del Directorio u Organismo que haga sus veces	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 políticas y estrategias relacionadas con la

															administración y gestión del riesgo operativo que permitan el cumplimiento de las disposiciones establecidas en este capítulo
		2. Procesos, procedimientos y metodologías alineados al cumplimiento de las políticas y estrategias de la administración del riesgo operativo aprobadas por el directorio: gestión de procesos, personas., tecnología de la información (incluye SGSI) y servicios provistos por terceros.		1				1					17.3	Podrá delegar la aprobación de los procesos, procedimientos y metodologías para la gestión de procesos, personas, tecnología de la información y servicios provistos por terceros a la instancia que considere pertinente, la misma que debe velar que los mismos estén alineados al cumplimiento de las políticas y estrategias de la administración del riesgo operativo aprobadas por el directorio
		3. Proceso, metodología y plan para la administración de la Continuidad del Negocio aprobado por el Directorio o quien haga sus veces.		1				1					17.4	Aprobar el proceso, metodología y plan para la administración de la continuidad del negocio.
	Funciones y responsabilidades del Comité de Administración Integral	**¿El Comité de Administración Integral de Riesgos cumple con las siguientes funciones y responsabilidades?..**											**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 de riesgos", del capítulo I "De la gestión integral y control de riesgos". Adicionalmente, el comité de administración integral de riesgos tendrá las siguientes responsabilidades en relación con la administracióndel riesgo operativo:**	
		1. Evaluar y proponer para la aprobación del directorio las políticas para		1				1				Reglamento del Comité de Administración	18.1	Evaluar y proponer para la aprobación del directorio las políticas para la

		la administración del riesgo operativo.											administración del riesgo operativo
		2. Evaluar y proponer mejoras al proceso de administración de riesgo operativo y asegurarse que sean implementados en toda la institución.		1			1				Integral de Riesgos	18.2	Evaluar y proponer mejoras al proceso de administración de 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
		3. Definir los mecanismos para monitorear y evaluar los cambios significativos y la exposición a riesgos		1			1					18.3	Definir los mecanismos para monitorear y evaluar los cambios significativos y la exposición a riesgos
		4. Evaluar y someter a aprobación del directorio el proceso, metodología y plan de continuidad del negocio de acuerdo a lo establecido en la Norma de la Superintendencia de Bancos.		1			1					18.4	Evaluar y someter a aprobación del directorio el proceso, metodología y plan de continuidad del negocio a los que se refiere la sección IV, del este capítulo; asegurar su aplicabilidad; y, cumplimiento del mismo
		5. Analizar y aprobar la designación de líderes encargados de llevar a cabo las actividades previstas en el plan de continuidad del negocio.		1			1					18.5	Analizar y aprobar la designación de líderes encargados de llevar a cabo las actividades previstas en el plan de continuidad delnegocio
	Funciones y responsabilidades de la unidad de riesgos en relación con la administración del riesgo operativo:	**¿La unidad de riesgos de la institución cumple las siguientes funciones y responsabilidades?..**											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".Adicionalmente, la unidad de riesgos tendrán las siguientes responsabilidades en relación con la administración del riesgo operativo:

		1. Diseñar las políticas y el proceso de administración del riesgo operativo		1				1					19.1	Diseñar las políticas y el proceso de administración del riesgo operativo
		2. Implementar un procedimiento para monitorear y evaluar los cambios significativos y la exposición a riesgos provenientes de los procesos, las personas, la tecnología de la información y los eventos externos.		1				1					19.2	Monitorear y evaluar los cambios significativos y la exposición a riesgos provenientes de los procesos, las personas, la tecnología de la información y los eventos externos;
		3. Presentar al CAIR propuestas de cada área respectiva: Políticas y procedimientos en función de los factores de riesgos (procesos, personas, eventos externos y tecnología de la información), especialmente aquellas relacionadas con la seguridad de la información		1				1				Manual de Funciones de la Unidad de Riesgos	19.3	Analizar las políticas y procedimientos propuestos por el área respectiva, para los procesos, personas, eventos externos y tecnología de la información, especialmente aquellas relacionadas con la seguridad de la información
		4. Desarrollar el proceso y plan de continuidad del negocio, verificar su aplicabilidad y cumplimiento: nombre de los líderes de las áreas, responsable del proceso de la administración de la continuidad y sus respectivas funciones.		1				1					19.4	Liderar el desarrollo, la aplicabilidad y cumplimiento del proceso y plan de continuidad del negocio, al que se refiere la sección IV de este capítulo; así como proponer el nombre de los líderes de las áreas que deban cubrir el plan de continuidad del negocio, para lo cual debe designar de manera formal, un responsable del proceso de la administración de la continuidad, el cual debe tener a su cargo, entre otras, las siguientes funciones:
		5. Políticas, procedimientos y metodologías para la administración de la continuidad del negocio, incluyendo la asignación		1				1					19.4.1	Proponer las políticas, procedimientos y metodologías para la administración de la continuidad del

		de roles y responsabilidades													negocio, incluyendo la asignación de roles y responsabilidades
		6. Presentar al CAIR propuestas de actualización, cambios y mejora del plan de continuidad de negocio.		1			1						19.4.2 y 19.4.3		Proponer cambios, actualizaciones y mejorar al plande continuidad. Informar al comité de continuidad los aspectos relevantes de la administración de la continuidad del negocio para una oportuna toma de decisiones.
		7. Riesgo Legal: análsis, monitoreo y evaluacion de procedimientos de orden legal de la institución: informes que determinen exposición al riesgo legal y comunicación al comité de administración integral de riesgos.		1			1						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.
			0	**15**	**0**	**0**	**0**	**15**							

CALIFICACION DE RIESGO	**1,00**	**bajo**

calificacion	riesgo
1	bajo
0	0
0	0
0	0
0	0

Nivel Riesgo	Rango Mínimo	Rango Máximo	Riesgo
Uno	0	1	bajo
Dos	1,01	1,75	medio bajo
Tres	1,76	2,5	medio
Cuatro	2,51	3,25	medio alto
Cinco	3,26	4	alto

EVALUACION ADMINISTRACION DE RIESGO OPERATIVO

APLICACIÓN DE NORMATIVA / CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO; TÍTULO X .- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, DEL LIBRO I.- NORMAS GENERALES PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO

SECCIÓN IV.- CONTINUIDAD DEL NEGOCIO			**De acuerdo al segmento que pertenece, colocar "1" si cumple o "0" si no cumple.**						**Si la respuesta es "No Cumple", completar datos del proyecto**					**NORMATIVA EXIGIBLE**
			n/a	**cumple**	**satisfactorio**	**parcialmente**	**no cumple**	**total**	Procentaje de Avance de implementación	Fecha proyecto		Area responsable	Referencia	
			0	**1**	**2**	**3**	**4**			Inicio	Fin			Detallar los requerimientos normativos exigibles a considerar para la verificación que la entidad cumple con lo estipulado.
CONTINUIDAD DE	Garantizar la capacidad de operación en forma continua y minimizar las pérdidas en caso	¿Cuenta la institución con un Plan de Continuidad de Negocio debidamente aprobado por el directorio u organismo que haga sus veces?.		**1**				1					Plan de Continuidad de Negocios	ARTÍCULO 15.- Las instituciones controladas deben administrar la continuidad del negocio, manteniendo procedimientos actualizados, a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción del negocio. Para el efecto, las instituciones del sistema financiero deben establecer un proceso de administración de la continuidad del negocio, tomando como referencia el estándar ISO 22301 o el que lo sustituya, y considerar al menos lo siguiente:
		El proceso de Administración de Continuidad del Negocio (de acuerdo al estándar ISO 22301 o el que lo sustituya) considera al menos lo siguiente:												

		a. Definición de objetivos, políticas, estrategias, procedimientos, metodología, planes y presupuesto para la administración de la continuidad.		1				1				Plan de Continuidad de Negocios, Certificación de Presupuesto Anual aprobado, Manual de Políticas y Procedimientos	15.1	La definición de objetivos, políticas, estrategias,procedimientos, metodología, planes y presupuesto para la administración de la continuidad
		b. Conformación del comité de continuidad del negocio, su reglamento, entre otros.		1				1				Reglamento del Comité	15.2	Un comité de continuidad del negocio que esté conformado como mínimo por los siguientes miembros: el funcionario responsable de la unidad de riesgos, quien lo preside, el funcionario responsable de la administración de la continuidad, quien hará las veces de secretario, el funcionario responsable del área de tecnología de la información, el funcionario responsable del área de talento humano, el auditor interno, solo con voz, y el máximo representante de cada una de las áreas involucradas en el proceso de administración de la continuidad. El comité de continuidad del negocio debe sesionar mínimo con la mitad más uno de sus integrantes, al menos una vez cada trimestre, ysus decisiones serán tomadas por mayoría absoluta de votos. El presidente del comité tendrá voto dirimente. El comité de continuidad del negocio debe dejar evidencia de las decisiones adoptadas, las cuales deben ser conocidas y aprobadas por el comité de administración integral de riesgos. El comité de continuidad del negocio debe tener al menos las siguientes

																responsabilidades: 15.2.1. Monitorear la implementación del plan y asegurar elalineamiento de éste con la metodología; y, velar por una administración de la continuidad del negocio competente 15.2.2. Proponer cambios, actualizaciones y mejoras al plan 15.2.3. Revisar el presupuesto del plan y ponerlo en conocimiento del comité de administración integral de riesgos. 15.2.4. Dar seguimiento a las potenciales amenazas que pudieran derivar en una interrupción de la continuidad de las operaciones y coordinar las acciones preventivas; 15.2.5. Realizar un seguimiento a las medidas adoptadas en caso de presentarse una interrupción de la continuidad de las operaciones
		c) **A**nálisis de **I**mpacto en el **N**egocio (BIA en inglés), generado por interrupción en los procesos que soportan los principales productos y servicios.		1			1					Análisis de Impacto en el Negocio	15.3	Análisis de impacto que tendría una interrupción de los procesos que soportan los principales productos y servicios. Para ello, deben determinar el impacto en términos de magnitud de daños, el período de recuperación y tiempos máximos de interrupción que puedan ocasionar los siniestros. El análisis de impacto debe ser revisado periódicamente y actualizado cuando existan cambios en la organización o en su entorno, que puedan afectar sus resultados.
		d) Metodología para identificar y analizar los principales escenarios de riesgos.		1			1					Metodología de Análisis de Riesgos	15.4	Análisis que identifique los principales escenarios de riesgos, incluyendo las fallas en la tecnología de la

														información, tomando en cuenta el impacto y la probabilidad de que sucedan. Para ello, debe seguirse una metodología consistente con aquella utilizada para la evaluación de los demás riesgos
		e) Evaluación y selección de estrategias de continuidad de negocios, que permitan reestablecer y/o mantener la ejecución de los procesos críticos que soportan los principales productos y servicios, dentro del tiempo objetivo de recuperación definido:		1				1				Plan de Continuidad de Negocios y de Contingencias	15.5	Evaluación y selección de estrategias de continuidad por proceso que permitan mantener la continuidad de los procesos que soportan los principales productos y servicios, dentro del tiempo objetivo de recuperación definido para cada proceso, mismas que deben tomar en cuenta, al menos lo siguiente: la seguridad del personal, habilidades y conocimientos asociados al proceso, instalaciones alternas de trabajo, infraestructura alterna de procesamiento e información que soporte el proceso, seguridad de la información y equipamiento necesario para el proceso
		f) Simulacros (al menos una vez al año) del plan de continuidad del negocio que permitan comprobar su efectividad y realizar los ajustes necesarios, cuando existan cambios que afecten la aplicabilidad del plan.		1				1				Informe de Pruebas realizadas	15.6	Realización de pruebas del plan de continuidad del negocio que permitan comprobar su efectividad y realizar los ajustes necesarios, cuando existan cambios que afecten la aplicabilidad del plan o al menos una (1) vez al año.
		g) Procedimientos de difusión, comunicación, entrenamiento y concienciación del plan y su cumplimiento.		1				1				Procedimientos	15.7	Procedimientos de difusión, comunicación, entrenamiento y concienciación del plan y su cumplimiento.
		h) Incorporación del proceso de Administración de la Continuidad del Negocio al Macroproceso Administración Integral de Riesgos.		1				1				Inventario de Procesos	15.8	Incorporación del proceso de administración de la continuidad del negocio al proceso de administración integral de riesgos, que garantice la actualización y mejora continúa del plan de continuidad del negocio.
		i) Procedimiento de actualización y mejora		1				1				Procedimientos		

		continúa del Plan de Continuidad del Negocio.														
	Plan de Continuidad del Negocio	**2. El <u>Plan de Continuidad del Negocio (PCN)</u> contiene al menos lo siguiente:**												ARTÍCULO 16.- El plan de continuidad del negocio debe contener al menos los procedimientos operativos, tecnológicos, de emergencias y comunicaciones para cada proceso crítico y para cada escenario cubierto, los cuales deben considerar, según corresponda, como mínimo lo siguiente:		
		a). Procesos críticos cubiertos y no cubiertos por el plan; determinar sus respectivos escenarios y alertas de riesgos.		1			1					Plan de Continuidad de Negocios	16.1	Escenarios de riesgos y procesos críticos cubiertos y alertas de los escenarios y procesos críticos no cubiertos por el plan
		b). Roles y responsabilidades de las personas encargadas de ejecutar cada actividad del plan.		1			1						16.2	Roles y responsabilidades de las personas encargadas de ejecutar cada actividad
		c). Criterios de invocación y activación del plan		1			1						16.3	Criterios de invocación y activación del plan
		d). Responsable de su actualización		1			1						16.4	Responsable de su actualización
		e). Acciones y procedimientos a ejecutar antes, durante y después de ocurrido el incidente que active el PCN.		1			1						16.5	Acciones y procedimientos a ejecutar antes, durante y después de ocurrido el incidente que ponga en peligro la operatividad de la institución, priorizando la seguridad del personal
		f). Tiempos máximos de interrupción y de recuperación de cada proceso		1			1						16.6	Tiempos máximos de interrupción y de recuperación de cada proceso
		g). Acciones y procedimientos para realizar las principales actividades y trasladar los procesos críticos a ubicaciones transitorias/alternativas o para su restablecimiento de manera urgente.		1			1						16.7	Acciones y procedimientos a realizar para trasladar las actividades de la institución a ubicaciones transitorias alternativaso para el restablecimiento de los procesos críticos de manera urgente
		h). Definir información vital y cómo acceder a ella: información de clientes,		1			1						16.8	Información vital y cómo acceder a ella (incluye información de clientes, contratos, pólizas de seguro,

		contratos, pólizas de seguro, manuales tècnicos y operativos, flujos de procesos que se activan, comunicación con personal crítico, contratos de emergencia, entre otros.												manuales técnicos y de operación, entre otros)
													16.9	Comunicaciones con el personal involucrado, sus familiares y contactos de emergencia, para lo cual debe contar con la información para contactarlos oportunamente (direcciones, teléfonos, correos electrónicos, entre otros);
		i). Interacción con los medios de comunicación		1			1						16.10	Interacción con los medios de comunicación
		j). Comunicación con los grupos de interés		1			1						16.11	Comunicación con los grupos de interés
		k). Establecimiento de un centro de comando (principal y alterno)		1			1						16.12	Establecimiento de un centro de comando (considerar al menos un sitio principal, y uno alterno)
		l). Procedimiento de restauración en una ubicación remota de los servicios de tecnología de la información (establecidos en el plan) y posterior recuperación de las condiciones previas a su ocurrencia. La ubicación remota no debe estar expuesta a los mismos riesgos del sitio principal.		1			1						16.13	Ante eventos de desastre en el centro principal de procesamiento, los procedimientos de restauración en una ubicación remota de los servicios de tecnología de la información deben estar dentro de los parámetros establecidos en el plan, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia. La ubicación remota no debe estar expuesta a los mismos riesgos del sitio principal.
			0	**22**	**0**	**0**	**0**	**22**						

CALIFICACION DE RIESGO	**1,00**	**bajo**

calificacion	riesgo
1	bajo
0	0
0	0
0	0
0	0

Nivel Riesgo	Rango Mínimo	Rango Máximo	Riesgo
Uno	0	1	bajo
Dos	1,01	1,75	medio bajo
Tres	1,76	2,5	medio
Cuatro	2,51	3,25	medio alto
Cinco	3,26	4	alto

GESTIÓN DEL RIESGO OPERATIVO

	ACTIVIDAD REQUERIDA	CALIFICACION DE RIESGOS						
		N/A	CUMPLE	SATISFACTORIO	PARCIALMENTE	NO CUMPLE	TOTAL	
		0	1	2	3	4		OBSERVACIONES
FACTOR - PROCESOS								
	ACTIVIDADES EVALUADAS	0	18	0	0	0	18	Puntos a Mejorar:
	TOTAL PUNTAJE	0	18	0	0	0	18	
	CALIFICACION DE RIESGO	1,00			bajo			
FACTOR - PERSONAS								
	ACTIVIDADES EVALUADAS	0	14	0	0	0	14	Puntos a Mejorar:
	TOTAL PUNTAJE	0	14	0	0	0	14	
	CALIFICACION DE RIESGO	1,00			bajo			
FACTOR - TI								
	ACTIVIDADES EVALUADAS	0	32	0	0	0	32	Puntos a Mejorar:
	TOTAL PUNTAJE	0	32	0	0	0	32	
	CALIFICACION DE RIESGO	1,00			bajo			
EXTERNOS Y SERVICIOS								
	ACTIVIDADES EVALUADAS	0	19	0	0	0	19	Puntos a Mejorar:
	TOTAL PUNTAJE	0	19	0	0	0	19	
	CALIFICACION DE RIESGO	1,00			bajo			
SEGURIDAD DE LA INFORMACIÓN								
	ACTIVIDADES EVALUADAS	0	27	0	0	0	27	Puntos a Mejorar:
	TOTAL PUNTAJE	0	27	0	0	0	27	

	CALIFICACION DE RIESGO	**1,00**			**bajo**			
ADMINISTRACIÓN INTEGRAL DE RIESGOS								
	ACTIVIDADES EVALUADAS	**0**	**21**	**0**	**0**	**0**	**21**	**Puntos a Mejorar:**
	TOTAL PUNTAJE	**0**	**21**	**0**	**0**	**0**	**21**	
	CALIFICACION DE RIESGO	**1,00**			**bajo**			
RESPONSABILIDAD DIRECCION								
	ACTIVIDADES EVALUADAS	**0**	**15**	**0**	**0**	**0**	**15**	**Puntos a Mejorar:**
	TOTAL PUNTAJE	**0**	**15**	**0**	**0**	**0**	**15**	
	CALIFICACION DE RIESGO	**1,00**			**bajo**			
CONTINUIDAD DEL NEGOCIO								
	ACTIVIDADES EVALUADAS	**0**	**22**	**0**	**0**	**0**	**23**	**Puntos a Mejorar:**
	TOTAL PUNTAJE	**0**	**22**	**0**	**0**	**0**	**22**	
	CALIFICACION DE RIESGO	**1,00**			**bajo**			
TOTAL ACTIVIDADES Y EVALUACIÓN FINAL								
	ACTIVIDADES EVALUADAS	**0**	**168**	**0**	**0**	**0**	**168**	**Puntos a Mejorar:**
	TOTAL PUNTAJE	**0**	**168**	**0**	**0**	**0**	**168**	
	CALIFICACION DE RIESGO LINEAL	**1,00**			**bajo**			
	CALIFICACION PONDERADA POR PESO	**1,00**			**bajo**			
	CALIFCACION ADMINISTRACION RIESGO OPERATIVO COAC ATUNTAQUI	**A**						

ANEXO D. Metodología Evaluación Riesgo Operativo aplicada a la COAC Atuntaqui Ltda.

GESTIÓN DEL RIESGO OPERATIVO

	ACTIVIDAD REQUERIDA	CALIFICACION DE RIESGOS						
		N/A	CUMPLE	SATISFACTORIO	PARCIALMENTE	NO CUMPLE	TOTAL	
		0	1	2	3	4		OBSERVACIONES
FACTOR - PROCESOS								
	ACTIVIDADES EVALUADAS	**0**	**3**	**10**	**5**	**0**	**18**	**Puntos a Mejorar:** Políticas claras que permitan la identificación de los procesos críticos y el diseño claro de los procesos establecidos en los manuales de normalización y estandarización.
	TOTAL PUNTAJE	**0**	**3**	**20**	**15**	**0**	**38**	
	CALIFICACION DE RIESGO	**2,11**			**medio**			
FACTOR - PERSONAS								
	ACTIVIDADES EVALUADAS	**0**	**3**	**7**	**4**	**0**	**14**	**Puntos a Mejorar:** Procesos de incorporación y permanencia.
	TOTAL PUNTAJE	**0**	**3**	**14**	**12**	**0**	**29**	
	CALIFICACION DE RIESGO	**2,07**			**medio**			
FACTOR - TI								
	ACTIVIDADES EVALUADAS	**0**	**15**	**6**	**8**	**3**	**32**	**Puntos a Mejorar:** Establecimiento de una metodología de administración de proyectos enfocada en la optimización de recursos y la gestión de riesgos. / Integrar un inventario de la infraestructura tecnológica, identificando ítem, registro, responsables de uso y mantenimiento. / Incorporar un Plan Operativo de necesidades tecnológicas.
	TOTAL PUNTAJE	**0**	**15**	**12**	**24**	**12**	**63**	
	CALIFICACION DE RIESGO	**1,97**			**medio**			
EXTERNOS Y SERVICIOS								
	ACTIVIDADES EVALUADAS	**0**	**1**	**0**	**6**	**12**	**19**	**Puntos a Mejorar:** Para mantener una adecuada administración de proveedores, la institución debe contar con un
	TOTAL PUNTAJE	**0**	**1**	**0**	**18**	**48**	**67**	

	CALIFICACION DE RIESGO	**3,53**			**alto**			manual de procesos que cumpla con Políticas, procesos y procedimientos elaborados y aplicados para selección, calificación y evaluación de los proveedores.
SEGURIDAD DE LA INFORMACIÓN								
	ACTIVIDADES EVALUADAS	**0**	**7**	**12**	**7**	**1**	**27**	**Puntos a Mejorar:** Establecer un Comité de Seguridad de la Información.
	TOTAL PUNTAJE	**0**	**7**	**24**	**21**	**4**	**56**	
	CALIFICACION DE RIESGO	**2,07**			**medio**			
ADMINISTRACIÓN INTEGRAL DE RIESGOS								
	ACTIVIDADES EVALUADAS	**0**	**6**	**7**	**2**	**6**	**21**	**Puntos a Mejorar:** Se debe establecer procedimientos que engloben las fallas o insuficiencias de orden legal enfocados en los siguientes campos: Actos Societarios, Gestión de Crédito, Operación del giro financiero, Actividades complementarias de las operaciones del giro financiero, Cumplimiento legal y normativo.
	TOTAL PUNTAJE	**0**	**6**	**14**	**6**	**24**	**50**	
	CALIFICACION DE RIESGO	**2,38**			**medio**			
RESPONSABILIDAD DIRECCION								
	ACTIVIDADES EVALUADAS	**0**	**6**	**6**	**2**	**1**	**15**	**Puntos a Mejorar: Es necesario el monitoreo y evaluación de procedimientos de orden legal de la institución: informes que determinen exposición al riesgo legal y comunicación al comité de administración integral de riesgos.**
	TOTAL PUNTAJE	**0**	**6**	**12**	**6**	**4**	**28**	
	CALIFICACION DE RIESGO	**1,87**			**medio**			
CONTINUIDAD DEL NEGOCIO								
	ACTIVIDADES EVALUADAS	**0**	**1**	**6**	**12**	**3**	**23**	**Puntos a Mejorar: Conformación del Comité de Continuidad de la Información.**
	TOTAL PUNTAJE	**0**	**1**	**12**	**36**	**12**	**61**	
	CALIFICACION DE RIESGO	**2,77**			**medio alto**			

TOTAL ACTIVIDADES Y EVALUACIÓN FINAL							
ACTIVIDADES EVALUADAS	0	42	54	46	26	168	Puntos a Mejorar: Hay factores específicos que es indispensable el análisis de riesgos, respecto a los servicios provistos por terceros, los de orden legal y los de continuidad del negocio.
TOTAL PUNTAJE	0	42	108	138	104	392	
CALIFICACION DE RIESGO LINEAL	2,33			medio			
CALIFICACION PONDERADA POR PESO	2,33			medio			
NIVEL DE RIESGO	cinco						
CALIFCACION ADMINISTRACION RIESGO OPERATIVO COAC ATUNTAQUI	C						

La Administración de Riesgo Operativo sugiere obvias deficiencias, muy probablemente relacionadas con el incumplimiento de algunos aspectos normativos. Hacia el futuro existe un considerable nivel de incertidumbre en el cumplimiento de los procedimientos para un correcto control del riesgo operativo, pero con la propuesta de proyectos o actualizaciones se puede alcanzar las mejoras a un corto o largo plazo.

ANEXO E. Entrevista Ing. Jorge Dilón Experto en Gestión de Riesgos

Entrevista Realizada al Ing. Jorge Dilón Gerente de la Calificadora de Riesgo Sociedad Latinoamericana SCR.

La presente entrevista se realizó vía telefónica con el Ing. Jorge Dilón el día miércoles 15 de marzo del 2017 vía telefónica debido a que el domicilió del entrevistado es en la ciudad de Guayaquil.

CUESTIONARIO

En qué consiste la actividad de las empresas Calificadora de Riesgos?

Las empresas calificadoras de Riesgo se dedican a emitir calificaciones de riesgo enfocadas en los productos financieros, valorando algunas condiciones como solvencia, morosidad, liquidez, gobierno corporativo, estas entidades valoran desde productos financieros, economías de varios países, con el objetivo de establecer el nivel de confianza de las empresas evaluadas, por tal motivo es trabajo de estas entidades es muy serio, ya que puede impactar en mercados y economías nacionales e internacionales. De acuerdo a los cambios en los indicadores de una entidad, ya sean cambios positivos o negativos la calificadora puede aumentar o disminuir la calificación de riesgo, con el fin de proveedor de información validad y confiable a los mercados financieros.

¿Cómo ve la actual Administración de Riesgos de la COAC Atuntaqui?

La Administración de Riesgos de la cooperativa al igual que la de otras entidades del segmento 1, que son las cooperativas más grandes del Ecuador, no han brindado la importancias que tienen los eventos de Riesgo Operativo, y su impacto a la entidad; da la razón debido a que hasta hace algunos años, las entidades de control no daban la importancia o el peso respectivo al riesgo operativo, pero asevera que en otros países y muy pronto en el Ecuador, será un tema de innovación en todo campo empresarial. De igual manera creo que las auditorias que se realizan en mención del Riesgo Operativo es muy superficial; por tal motivo la Coac Atuntaqui maneja controles que otras entidades no tienen, pero no estoy seguro si internamente conocen de manera cuantificada el nivel de gestión de Riesgo Operativo.

¿Qué ponderación o peso le da al Riesgo Operativo?

Esto es algo subjetivo y de opinión, porque depende de la empresa en la cual se analice, particularmente creo que hay ciertas personas expertas en Riesgo, cuyo fuerte no es el operativo, y no le dan la importancia adecuada, personalmente soy una persona que conoce ampliamente la gestión de Riesgos, y he tenido la oportunidad de trabajar en empresas de diferente mercado, pero algo que siempre está presente y puede ser los mimos, son los eventos de riesgo operativo, te pongo un ejemplo, un terremoto, para enfrentarlo las estrategias que se deben aplicar son semejantes.

¿Qué recomendación podría dar respecto a la administración del Riesgo Operativo en la COAC Atuntaqui?

Mi recomendación seria la mejora continua, la capacitación constante en el campo del Riesgo Operativo, si bien Uds., están regidos por la SEPS, este organismo no maneja a profundidad muchos temas, entre esos el Riesgo Operativo, les recomiendo analicen la normativa expedida por la Superintendencia de Bancos.

¿Cuáles son las bases para una correcta Administración de Riesgo Operativo?

Las bases para una correcta administración es identificar el estado actual de Administración de Riesgo Operativo, no puedes implementar algo, o proponer algo sino conoces como te encuentras actualmente, que tienes, hasta donde tienes, para verificar si aplicando proyectos, o reformas se mejora en algo la administración, pero necesitan conocer o autoevaluarse internamente.

¿Qué normas son indispensables analizar para interpretar de manera correcta la Administración del Riesgo Operativo?

Existen varias normas, pero si deseas partir con una norma que contemple los aspectos fundamentales de Riesgo Operativo es la resolución 834, del libro de Administración de Riesgo Operativo expedido por la Superintendencia de Bancos y Seguros.

Entrevista realizada por el Ing. Ronald Macías