



**UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE CIENCIAS ADMINISTRATIVAS Y
ECONÓMICAS**

CARRERA DE INGENIERÍA EN CONTABILIDAD Y AUDITORÍA

INFORME FINAL DE TRABAJO DE GRADO

TEMA:

“MANUAL DE RIEGO OPERATIVO PARA MUTUALISTA IMBABURA”

**PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN
CONTABILIDAD Y AUDITORÍA C.P.A.**

AUTOR: FLORES, S. Carlos S.

DIRECTOR: Dr. LARA, Eduardo.

IBARRA, ABRIL DEL 2013

RESUMEN EJECUTIVO

El presente proyecto está orientado principalmente a definir la gestión de riesgo operativo en la Mutualista Imbabura, de la ciudad de Ibarra, el mismo que consiste en la elaboración de un manual de políticas y gestión de riesgo operativo, empezando mediante un diagnóstico previo que se obtuvo a través de entrevistas y encuestas a los directores y funcionarios de la institución, con la finalidad directa de detectar las fortalezas, oportunidades, debilidades y amenazas inherentes en las actividades diarias que se realizan; y con la información receptada, se efectuó un análisis para la elaboración propuesta de una gestión de riesgo eficaz y efectiva. Se formularon las normas básicas, políticas y procedimientos que deban utilizarse, estableciendo niveles de control interno y revisión que están reflejados a través de un organigrama estructural y funcional, se definen los principales temas relacionados con riesgo operativo y se fijan las políticas y procedimientos para finalmente especificar las funciones y responsabilidades de Directivos y Funcionarios en cuanto a los procesos internos, personas, tecnología de la información y factores externos. De esta manera se busca asegurar un adecuado y completo ámbito de control y mitigación de eventos de riesgo operativo. Se realizó un análisis detallado de los mecanismos de control con los que cuenta la Mutualista Imbabura con el fin de regularizar todos los procesos enmarcándolos en un ambiente de control y gestión de riesgo operativo, esto se logró con la aplicación de las técnicas específicas de investigación y con la ayuda de fuentes bibliográficas, con definiciones teóricas, con la ayuda de expertos y el sustento de las leyes y decretos vigentes. Se analizaron técnicamente los impactos que genera este proyecto mediante matrices indicadoras y niveles de conducción, por cada área o ámbito, siendo esto: Socio-cultural, económico y educativo.

EXECUTIVE SUMMARY

This project is aimed primarily at defining operational risk management in the Mutual Imbabura, Ibarra city, the same as is the development of a manual of policies and operational risk management, starting with a previous diagnosis was obtained through interviews and surveys to the directors and officers of the institution, with the direct purpose of identifying strengths, weaknesses, opportunities and threats inherent in daily activities that are performed, and receipted information, analysis was performed for the development proposed risk management efficiently and effectively. He formulated the basic rules, policies and procedures to be used, establishing levels of internal control and review are reflected through a structural and functional organization, identifies key issues and fixing operational risk policies and procedures to finally specify the roles and responsibilities of Directors and Officers in terms of internal processes, people, information technology and external factors. In this way it seeks to ensure full and appropriate level of control and mitigation of operational risk events. We performed a detailed analysis of the control mechanisms with which Imbabura Mutual account in order to regularize all processes framing them in a control and operational risk management, this was achieved with the application of specific research techniques and with the help of literature sources, with theoretical definitions, with the help of experts and the support of the laws and decrees in force. Technically were analyzed impacts generated by this project using indicator matrices and driving levels for each area or field, being this: Socio-cultural, economic and educational.

DECLARACIÓN

YO DECLARO BAJO JURAMENTO QUE EL TRABAJO AQUÍ DESCRITO "MANUAL DE RIESGO OPERATIVO PARA MUTUALISTA IMBABURA" ES DE MI AUTORÍA, QUE NO HA SIDO PREVIAMENTE PRESENTADO PARA NINGÚN GRADO NI CALIFICACIÓN PROFESIONAL Y QUE HE CONSULTADO E INVESTIGADO LAS REFERENCIAS BIBLIOGRÁFICAS QUE SE INCLUYEN EN ESTE DOCUMENTO.

A handwritten signature in blue ink, consisting of several loops and a horizontal line at the bottom, positioned above the printed name.

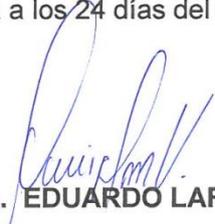
SANTIAGO FLORES

C.C 100251185-3

INFORME DE DIRECTOR DE TRABAJO DE GRADO

En mi calidad de Director del Trabajo de Grado presentado por el egresado Flores Sánchez Carlos Santiago para optar por el Título de Ingeniera en Contabilidad y Auditoría C.P.A., cuyo tema es "MANUAL DE RIESGO OPERATIVO PARA MUTUALISTA IMBABURA". Considero que el presente trabajo reúne los 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 24 días del mes de Abril del 2013



DR.CPA. EDUARDO LARA V. MSC
C.C 100074831-7
DIRECTOR DE TESIS

**CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A
FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE**

Yo, **Flores Sánchez Carlos Santiago** con cédula de ciudadanía N° 100251185-3, 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 de la obra o trabajo de grado denominado "**MANUAL DE RIESGO OPERATIVO PARA MUTUALISTA IMBABURA**" que ha sido desarrollado para optar por el título de **INGENIERO EN CONTABILIDAD Y AUDITORIA C.P.A.** en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo 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.

Firma: 
Nombre: Flores Sánchez Carlos Santiago
Cédula: 100251185-3

En la ciudad de Ibarra a los 24 días del mes de Abril del 2013

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 Reposición Digital Institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, decencia 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 información siguiente:

DATOS DE CONTACTO			
CÉDULA DE CIUDADANÍA:	DE	100251185-3	
APELLIDOS Y NOMBRES:	Y	Flores Sánchez Carlos Santiago	
DIRECCIÓN:	Parroquia Caranqui, Hernán Gonzales de Saa y Juana Atabalipa, Sector 4 esquinas		
EMAIL:	santysj@hotmail.com		
TELÉFONO FIJO:	062 650023	TELÉFONO CELULAR:	0991509236

DATOS DE LA OBRA	
TÍTULO:	Manual de Riesgo Operativo para Mutualista Imbabura
AUTOR:	Flores Sánchez Carlos Santiago
FECHA:	Abril del 2013
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	<input checked="" type="checkbox"/> PREGRADO <input type="checkbox"/> POSGRADO
TÍTULO POR EL QUE OPTA	Ingeniero en Contabilidad y Auditoría C.P.A.
ASESOR/DIRECTOR:	Dr. Eduardo Lara

2. AUTORIZACIÓN DE USO DE LA UNIVERSIDAD

Yo, Flores Sánchez Carlos Santiago, portador de la cedula de ciudadanía N° 100251185-3, en calidad de autor y titular de los

derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso de 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 investigación es original y se la desarrolló sin violar derechos de autor de terceros, por lo tanto la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrán en defensa de la Universidad en caso de reclamación por parte de terceros.

En la ciudad de Ibarra a los 24 días del mes de Abril del 2013.

EL AUTOR

Firma: 
Nombre: Flores Sánchez Carlos Santiago
Cédula: 100251185-3

ACEPTACIÓN

Firma: 
Nombre: Ing. Betty Chávez
Cargo: JEFE DE BIBLIOTECA

Facultado por resolución del Consejo Universitario

DEDICATORIA

El presente trabajo se lo dedico en primer lugar a Dios, por haberme dado la vida y permitirme culminar con éxito mi carrera, en segundo lugar a mis padres por sus esfuerzos para sacarme adelante aun en momentos de dificultad; en especial dedico este logro a mi madre Marcela Sánchez quien hizo de mi una persona de bien gracias a sus cuidados y controles, guiándome siempre por el camino del bien sin permitirme en ningún momento decaer y apoyándome con su amor en los momentos en los que yo la necesité. Por último dedico este trabajo a mi Director de tesis el Dr. Eduardo Lara quien con muy buena voluntad asumió la responsabilidad de guiarme en este trabajo de último momento.

Carlos Santiago

AGRADECIMIENTO

En el presente trabajo, quiero expresar mi agradecimiento a Dios por haberme permitido cumplir una meta más en mi vida, a mis padres quienes me dieron una carrera profesional con la cual podré mantenerme y forjar un futuro digno.

A la Universidad Técnica del Norte, por haberme abierto las puertas del camino de la sabiduría y formarme como un ser comprometido al aporte y desarrollo de la colectividad, a mis maestros que supieron inculcarme todos sus conocimientos, de manera especial al Dr. Eduardo Lar. Director de Tesis quien supo guiarme con sus conocimientos en el desarrollo del presente trabajo de grado.

Carlos Santiago

ÍNDICE GENERAL

RESUMEN EJECUTIVO	II
EXECUTIVE SUMMARY	III
DECLARACIÓN	¡ERROR! MARCADOR NO DEFINIDO.
INFORME DE DIRECTOR DE TRABAJO DE GRADO	¡ERROR! MARCADOR NO DEFINIDO.
CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE.....	¡ERROR! MARCADOR NO DEFINIDO.
AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA.....	VII
DEDICATORIA	IX
AGRADECIMIENTO	X
ÍNDICE GENERAL.....	XI
CAPÍTULO I.....	1
1. DIAGNÓSTICO ORGANIZACIONAL E INSTITUCIONAL.....	1
1.1 ANTECEDENTES.....	1
1.2 JUSTIFICACIÓN.....	3
1.3 OBJETIVOS DEL DIAGNÓSTICO.....	4
1.3.1 Objetivo General	4
1.3.2 Objetivos Específicos.....	5
1.4 VARIABLES DIAGNOSTICAS	5
1.4.1 Variables.....	5
1.4.2 Indicadores.....	6
1.4.2.1 Estructura administrativa.....	6
1.4.2.2 Procesos.....	6
1.4.2.3 Gestión de riesgos.....	6
1.4.2.4 Administración de talento humano.....	6
1.4.2.5 Fuentes de exposición al riesgo.....	7
1.4.2.6 Tecnología	7
1.4.2.7 Controles implementados	7

1.5. VARIABLES DIAGNÓSTICAS.....	8
1.5.1 Matriz de relación diagnóstica.....	8
1.6 MECÁNICA OPERATIVA.....	9
1.6.1 Identificación de la población.....	9
1.6.2 Cálculo de la muestra.....	9
1.6.3 Información primaria.....	9
1.6.4 Información Secundaria.....	10
1.6.5 Diseño de instrumentos investigativos.....	10
1.7 EVALUACIÓN DE LA INFORMACIÓN OBTENIDA.....	10
1.7.1. Entrevista al Jefe de Recursos Humanos.....	11
1.7.2. Entrevista al Auditor Interno.....	14
1.7.3. Entrevista al Jefe de Sistemas.....	16
1.7.4. Entrevista al Directorio, Representantes y Gerencia General.....	19
1.7.5. Encuesta dirigida al personal operativo y de soporte.....	22
1.8 CONSTRUCCIÓN DE LA MATRIZ FODA.....	30
1.9 EVALUACIÓN DE INFORMACIÓN ESTRATÉGICA FA, FO, DO, DA.	31
1.10 IDENTIFICACIÓN DE PROBLEMAS EN RELACIÓN CAUSA EFECTO.....	32
CAPÍTULO II.....	34
2. MARCO TEÓRICO.....	34
2.1 ENTIDADES FINANCIERAS.....	34
2.2 TIPOS DE ENTIDADES FINANCIERAS.....	34
2.3 ENTIDADES DE CONTROL DE INSTITUCIONES FINANCIERAS EN EL ECUADOR.....	35
2.4 DESCRIPCIÓN DE MUTUALISMO.....	35
2.4.1 Mutualista Imbabura.....	36
2.4.2 Organización de Mutualista Imbabura.....	36
2.4.3 Principios del Mutualismo.....	37
2.5 RIESGO.....	38
2.5.1 Conceptos y definiciones.....	38

2.5.2 Clasificación de los riesgos.....	39
2.5.2.1 Riesgo de crédito.....	39
2.5.2.2 Riesgo de mercado.....	40
2.5.2.3 Riesgo de tasa de interés y riesgo de tipo de cambio.....	40
2.5.2.4 Riesgo de liquidez.....	41
2.5.2.5 Riesgo operativo.....	41
2.5.2.6 Riesgo legal.....	42
2.5.2.7 Riesgo de reputación.....	43
2.8 FACTORES DE RIESGO OPERATIVO.....	43
2.8.1 Procesos.....	44
2.8.1.1 Procesos gobernantes o estratégicos.....	44
2.8.1.2 Procesos productivos, fundamentales u operativos.....	44
2.8.1.3 Procesos habilitantes, de soporte o apoyo.....	44
2.8.2 Personas.....	46
2.8.2.1 Los procesos de incorporación.....	46
2.8.2.2 Los procesos de permanencia.....	46
2.8.2.3 Los procesos de desvinculación.....	47
2.8.3 Tecnología de la Información.....	47
2.8.4 Factores externos.....	54
2.9 Identificación de riesgos.....	54
2.9.1 Riesgos Internos.....	54
2.9.2 Riesgos externos.....	54
2.10 LÍNEAS DE NEGOCIO.....	55
2.11 MEDICIÓN DE RIESGO OPERATIVO.....	56
2.11.1 Método del indicador básico BIA.....	56
2.11.2 Método estándar.....	57
2.11.3 Método de medición avanzada AMA.....	57
2.12 TEMAS RELACIONADOS A RIESGO OPERATIVO.....	59
2.12.1 Planes de continuidad del negocio.....	59
2.12.2 Planes de seguridad de la Información.....	60
2.12.3 Planes de contingencia.....	62
2.13 TEMAS RELACIONADOS AL PROYECTO DE TESIS.....	63

2.13.1 Diagnóstico.	63
2.13.2 Análisis de impactos.	64
CAPÍTULO III	65
3 PROPUESTA.....	65
3.1 INTRODUCCIÓN.....	65
3.2 GENERALIDADES.	66
3.2.1 Objetivo general.....	66
3.2.2 Objetivos específicos.....	66
3.3.3 Alcance.....	66
3.4 POLÍTICAS PARA LA ADMINISTRACIÓN DE RIESGO OPERATIVO.	67
3.4.1 Política General.	67
3.4.2 Políticas específicas.	67
3.4.3 Políticas aplicables a la generación del árbol de procesos.....	69
3.4.4 Políticas aplicables a la identificación de riesgos.....	69
3.4.5 Políticas aplicables a la selección del método de evaluación de riesgos.	70
3.4.6 Políticas aplicables a la identificación de controles y mitigaciones.	71
3.4.7 Políticas aplicables al análisis de riesgos.	72
3.4.8 Políticas aplicables a la evaluación del riesgo operativo.	73
3.4.9 Políticas aplicables al tratamiento de los riesgos.....	74
3.4.10 Políticas aplicables al monitoreo de los riesgos.....	75
3.4.11 Políticas aplicables a la comunicación y divulgación de resultados.	76
3.4.12 Políticas aplicables a la gestión para la creación de nuevos productos y servicios.	77
3.4.13 Políticas aplicables a la capacitación.....	77
3.5 FUNCIONES Y RESPONSABILIDADES DE LA ORGANIZACIÓN. ...	80
3.5.1 Del Directorio de Mutualista Imbabura.....	80
3.5.2 Funciones.	82
3.5.3 Comité de Riesgos.....	83
3.5.3.1 Integrantes.....	83

3.5.3.2 Funciones.	84
3.5.4 Unidad de Riesgos.....	85
3.5.4.1 Funciones.	85
3.6 PROCESO GENERAL PARA LA ADMINISTRACIÓN DE RIESGO OPERATIVO.....	86
3.6.1 Etapa de Identificación de los Factores de Riesgo operativo:.....	88
3.6.2 Etapa de Medición de los Factores de Riesgo.....	88
3.6.3 Etapa de Control/Mitigamiento de Riesgos operativos	89
3.6.4 Etapa de Monitoreo de Riesgos.....	90
3.7 GESTIÓN METODOLÓGICA Y PROCEDIMIENTOS ESPECÍFICOS DE RIESGO OPERATIVO.	91
3.8 ÁRBOL DE PROCESOS.....	94
3.8.1 Identificación.....	94
3.8.2 Catalogación.....	96
3.8.3 Procedimiento.....	96
3.8.4 Documentación.....	98
3.9 IDENTIFICACIÓN DE RIESGOS.....	98
3.9.1 Clasificación de Factores de Riesgo Operativo.....	99
3.9.2 Tipos de Eventos.....	99
3.9.3 Procedimiento.....	100
3.9.4 Documentación.....	101
3.10 SELECCIÓN DEL MÉTODO DE ANÁLISIS PARA LA EVALUACIÓN DE RIESGOS.....	102
3.10.1 Disponibilidad de la información.....	102
3.10.2 Análisis de calidad de datos.....	102
3.10.3 Tipos de análisis.....	103
3.10.4 Procedimiento.....	104
3.10.5 Documentación.....	105
3.11 CONTROL DEL RIESGO.....	105
3.11.1 Controles.....	106
3.11.2 Métodos de control.....	107
3.11.3 Mitigaciones.....	108

3.11.4 Procedimiento.....	109
3.11.5 Documentación.....	111
3.12 ANÁLISIS DEL RIESGO.....	112
3.12.1 Probabilidad de ocurrencia.....	113
3.12.2 Procedimiento.....	113
3.12.3 Severidad.....	117
3.12.4 Procedimiento.....	117
3.12.5 Solidez de los controles.....	120
3.12.6 Diseño.....	121
3.12.6.1 Eficiencia.....	121
3.12.7 Mapa de riesgos brutos.....	122
3.12.8 Mapa de riesgos residuales.....	124
3.13 VALORACIÓN DEL RIESGO.....	126
3.13.1 Valoración cuantitativa.....	126
3.13.1.1 Cuantificación de las pérdidas.....	126
3.13.1.2 Base de datos de eventos y pérdidas.....	128
3.13.1.3 Base de datos mínima.....	129
3.13.2 Métodos de cuantificación.....	131
3.14 TRATAMIENTO DEL RIESGO.....	131
3.14.1 Planteo general.....	131
3.14.2 Procedimiento.....	132
3.14.3 Documentación.....	134
3.15 MONITOREO.....	134
3.15.1 Planteamiento general.....	135
3.15.2 Procedimiento.....	137
3.15.3 Documentación.....	139
3.16 COMUNICACIÓN.....	139
3.16.1 Sistemas de información y comunicación.....	140
3.16.2 Procedimiento.....	141
3.17 MODELO DE GESTIÓN DE RIESGOS PARA NUEVOS NEGOCIOS Y PRODUCTOS.....	142
3.17.1 Procedimiento.....	143

3.17.2 Documentos de descargo.	144
3.18 CAPACITACIÓN.	144
3.18.1 Procedimiento.	145
3.18.2 Documentos de descargo.	146
CAPITULO IV.....	147
4 ANÁLISIS DE IMPACTOS	147
4.1 Bases teóricas.	147
4.2 IDENTIFICACIÓN DE LOS IMPACTOS.	148
4.2.1 Impacto en Procesos.	148
4.2.2 Impacto en Personas.	149
4.2.3 Impacto en tecnología de Información.	150
CONCLUSIONES Y RECOMENDACIONES	153
1. CONCLUSIONES.....	153
2. RECOMENDACIONES.....	155
GLOSARIO DE TÉRMINOS UTILIZADO EN EL MANUAL.....	156
BIBLIOGRAFÍA.....	160
LINCOGRAFÍA.....	162
ANEXOS.....	163
ENTREVISTA CON LA GERENCIA GENERAL DE MUTUALISTA IMBABURA.	163
ENTREVISTA CON EL JEFE DE RECURSOS HUMANOS DE MUTUALISTA IMBABURA.....	164
ENTREVISTA CON LA AUDITORA INTERNA DE MUTUALISTA IMBABURA.	166
ENTREVISTA CON EL JEFE DE SISTEMAS DE MUTUALISTA IMBABURA.	167
ENCUESTA ANÓNIMA DIRIGIDA AL PERSONAL OPERATIVO Y DE SOPORTE DE LA MUTUALISTA IMBABURA.....	168

ÍNDICE DE CUADROS

Cuadro No. 1. Matriz de relación diagnóstica.	8
Cuadro No. 2. Matriz FODA.....	30
Cuadro No. 3. CRUCES ESTRATÉGICOS.	31
CUADRO No 4. Organigrama de Mutualista Imbabura.....	37
Cuadro No. 5. Proceso específicos para la administración de R O.	55
Cuadro No. 6. Requerimientos métodos de medición.	58
Grafico No. 7. Seguridad de la información.	61
Cuadro No. 8. Ejemplo de levantamiento de riesgos.....	63
Cuadro No. 9. Formato de evaluación Políticas específicas.....	68
Cuadro No. 10. Formato de evaluación Políticas específicas.....	79
Cuadro No. 11. Proceso general para la administración de R O.	87
Cuadro No. 12. Proceso específicos para la administración de R O.	93
GRAFICO No. 13 Árbol de procesos.	95
Cuadro No. 14. Procedimiento árbol de procesos	96
Cuadro No. 15. Procedimiento identificación de riesgos.....	100
Cuadro No. 16. Procedimiento para el análisis de riesgos	104
Cuadro No. 17. Procedimiento de control de riesgos	109
Cuadro No. 18. Procedimiento de análisis riesgos	113
CUADRO No 19. Ejemplo de Histograma.....	115
CUADRO No 20. Ejemplo de cálculo.....	116
Cuadro No. 21. Procedimiento de Análisis de riesgos	117
CUADRO No 22. Ejemplo de cálculo.....	118
CUADRO No 23. Ejemplo de cálculo.....	119
GRAFICO No. 24. Mapa de riesgos brutos.....	124
GRAFICO No. 25. Matriz de controles.....	125
GRAFICO No. 26. Mapa de riesgos residual	126
Cuadro No. 27. Procedimiento de tratamiento de riesgos.	133
Cuadro No. 28. Procedimiento de Monitoreo de riesgos.	137

Cuadro No. 29. Procedimiento de comunicación de información de riesgos.	141
Cuadro No. 30. Procedimiento de modelo de gestión para nuevos productos	143
Cuadro No. 31. Procedimiento de capacitación de riesgo operativo	145
CUADRO No 32. Cuantificación de impactos	147
CUADRO No 33 Matriz de valoración.....	148
CUADRO No 34 MATRIZ DE IMPACTO EN PROCESOS	149
CUADRO No 35 MATRIZ DE IMPACTO EN PERSONAS	150
CUADRO No 36 MATRIZ DE IMPACTO EN TECNOLOGÍA DE INFORMACIÓN	151
CUADRO No 37 MATRIZ DE GENERAL	152

CAPÍTULO I.

1. DIAGNÓSTICO ORGANIZACIONAL E INSTITUCIONAL.

1.1 ANTECEDENTES.

La ciudad de Ibarra capital de la provincia de Imbabura es considerada la ciudad más joven del Ecuador por su refundación en 1872 luego de un fatal terremoto que arrasó con casi la totalidad de sus viviendas y ocasionó la muerte de las tres cuartas partes de sus pobladores. Desde su reconstrucción hasta la presente fecha la ciudad ha venido creciendo y desarrollándose económicamente lo que ha permitido el asentamiento de algunas instituciones financieras como Bancos, Cooperativas de Ahorro y Crédito, Mutualistas y Sociedades Financieras que se dedican a la intermediación y a la administración de los recursos de la población económicamente activas.

Las Mutualistas se crearon por Decreto Ejecutivo publicado en Registro oficial No. 223 del 26 de mayo de 1961, considerando para su constitución el elevado déficit habitacional existente en el Ecuador y la imposibilidad de que el Banco Ecuatoriano de la Vivienda como entidad estatal pueda satisfacer dichas necesidades. La naturaleza y objetivo social de estas entidades se revalida en el artículo 2 de la Ley General de Instituciones del Sistema Financiero actualmente en vigencia que establece: "Las Asociaciones Mutualistas de Ahorro y Crédito para la Vivienda son instituciones cuya actividad principal es la captación de recursos del público para destinarlos al financiamiento de la vivienda, la construcción y el bienestar social de sus asociados, que deberá evidenciarse en la composición de sus activos", Ley promulgada del 12 de mayo de 1994 y cuyo reglamento fue emitido el 4 de julio del mismo año.

Existen cuatro mutualista a nivel nacional de las cuales dos operan en la ciudad de Ibarra, entre ella MUTUALISTA IMBABURA cuya creación, según datos históricos, data de la década del sesenta, por inquietud de un grupo de personas encabezadas por el Rvdo. Padre Honorato Cobo, nace la idea de formar una Mutualista en la provincia de Imbabura, para lo cual proceden a elaborar los estatutos que regirán a esta entidad, los mismos que son enviados al Banco Ecuatoriano de la vivienda, entidad que estaba facultada para aprobar y autorizar que opere Mutualista Imbabura.

El 19 de noviembre de 1963, luego de cumplir con todos los requerimientos necesarios el Banco Ecuatoriano de la Vivienda, en la persona del Sr. Ing. Alfredo Albornoz Andrade en su calidad de Gerente General, procede a aprobar sin modificación alguna los Estatutos ordenando su suscripción en el Registro del Banco. En vista de haber cumplido con todos y cada uno de los requerimientos legales, otorga a Mutualista Imbabura a la carta constitutiva la misma que autoriza operar en el país de conformidad a las normas legales pertinentes.

El 8 de diciembre de 1963, se llama a la primera sesión de junta General de Asociados con el fin de nombrar Directores principales y suplentes los mismos que regirán los destinos de la Mutualista, siendo nombrados los señores: Dr. Honorato Cobo, como Presidente, Dr. Carlos Villacís G., Dr. Horacio Yapes M., y Sr. Jorge Aníbal Páez P., en sus calidades de vocales Principales. De esta manera hasta la presente fecha Mutualista Imbabura ha venido sirviendo incesantemente a la ciudadanía de la sierra norte del país debido a que cuenta con tres oficinas las mismas que se encuentran ubicadas en la Ciudad de Ibarra (oficina matriz), la Agencia Otavalo y la Sucursal Quito.

La denominada unidad integral de riesgos es la dependencia interna encargada del control de todos los riesgos en la institución y no cuenta con un manual de políticas, procesos y metodologías para la

administración de riesgo operativo, fue creada en el año 2004 por requerimiento de la Superintendencia de Bancos debido a que las instituciones únicamente mantenían consultorías externas sobre riesgos

Un manual de riesgo operativo en la Mutualista Imbabura, según requerimiento de la Superintendencia de Bancos y Seguros, organismo rector de las instituciones financieras, permite a la misma administrar los riesgos identificados en todas las áreas de la institución, así como el adecuado uso y mantenimiento de los recursos existentes como son: Recurso Humano, Recurso Económico y Recursos Tecnológicos según lo señala el Capítulo V De la Gestión de Riesgo Operativo incluido con la resolución No. JB-2005-834 de 20 de Octubre del 2005.

Es así que Mutualista Imbabura mantiene siempre un estricto control y manejo de los diferentes riesgos a los que se enfrenta día a día por el giro de su actividad económica independientemente que sean factores internos o externos los que perjudiquen a la institución.

1.2 JUSTIFICACIÓN.

El negocio bancario es un negocio de riesgos, los mismos que pueden ocasionar la quiebra de las instituciones financieras si no se cuenta con herramientas que permitan monitorear y controlar los riesgos inherentes en las actividades financieras. Existen varios tipos de riesgos que desde la creación del Comité de Basilea se han empezado a controlar, como es el caso del Riesgo de Crédito, Riesgo de Liquidez y Mercado, Riesgo legal, Riesgo Estratégico, siendo estos riesgos los que involucran únicamente a ciertas áreas de la institución. El Riesgo Operativo está implícito en todas y cada una de las actividades, áreas y procesos que se realice en la institución y su administración es considerada complicada y

extensa por la magnitud de eventos de riesgo que se derivan de las operaciones diarias.

Es importante la implementación del Manual de Riesgo Operativo en la Mutualista Imbabura debido a que es necesario establecer esquemas eficientes y efectivos de administración y control de todos los eventos de riesgo operativo a los que se encuentra expuesta la institución, así como también, contar con procesos formales de administración del riesgo que permitan identificar, medir, controlar / mitigar y monitorear las exposiciones de riesgos que se están asumiendo.

Otro factor por el que es importante implantar el Manual de Riesgo Operativo en Mutualista Imbabura es para dar cumplimiento a lo señalado en la resolución No. JB-2005-834 de 20 de Octubre del 2005, emitida por la Superintendencia de Bancos y Seguros, en donde se exige a las instituciones financieras controladas por este organismo desarrollen un plan de gestión de riesgo operacional el mismo que deberá ser diseñado de acuerdo a necesidad de cada institución, como fecha máxima el 31 de octubre del 2009.

Debido a la importancia que este proyecto posee, la información y realización del mismo se apega a hechos reales, los mismos que son suficientes, oportunos y confiables sobre el manejo de los recursos de Mutualista Imbabura. El presente proyecto propone una adecuada administración de los eventos de riesgo evitando pérdidas económicas y altas provisiones de capital.

1.3 OBJETIVOS DEL DIAGNÓSTICO

1.3.1 Objetivo General

Determinar si se cuenta con políticas y procedimientos para una adecuada administración del riesgo operativo en la que se contemple

todos los factores, procesos, personas, tecnología de información y aspectos externos, estableciendo un manual de riesgo operativo para la Mutualista Imbabura.

1.3.2 Objetivos Específicos

- Verificar una adecuada estructura orgánica funcional de la Unidad de riesgos dentro de la institución.
- Analizar los procesos con los que cuenta la institución para el desarrollo de sus operaciones diarias.
- Evaluar la gestión de riesgo operativo efectuada por las diferentes áreas de la institución las cuales son las encargadas de su control y seguimiento.
- Determinar el grado de conocimiento sobre riesgo operativo del personal con el que cuenta la Mutualista.
- Definir las fuentes de exposición de riesgo operativo en base a la información levantada por la institución.
- Determinar el nivel de tecnología con el que cuenta la institución para la medición de Riesgo operativo.
- Determinar los controles implementados para la prevención de los riesgos operativos.

1.4 VARIABLES DIAGNOSTICAS

1.4.1 Variables.

- Estructura orgánica funcional

- Levantamiento de procesos.
- Gestión de riesgos.
- Administración de talento humano
- Fuentes de exposición al riesgo
- Tecnología de información
- Controles Implementados

1.4.2 Indicadores.

1.4.2.1 Estructura administrativa.

- Estructura Orgánica
- Funciones
- Perfiles

1.4.2.2 Procesos.

- Gobernantes
- Productivos
- Habilitantes

1.4.2.3 Gestión de riesgos.

- Fallas en Procesos
- Fallas de Personas
- Fallas de Tecnología de la información
- Continuidad del Negocio.
- Procesos provistos por terceros

1.4.2.4 Administración de talento humano

- Vinculación,
- Permanencia,

- Motivación,
- Promoción,
- Desvinculación.

1.4.2.5 Fuentes de exposición al riesgo

- Mecanismos de levantamiento de información,
- Frecuencia de reportes.

1.4.2.6 Tecnología

- Sistema implementado,
- Bases de datos de eventos.

1.4.2.7 Controles implementados

- Controles concurrentes y posteriores.

1.5. VARIABLES DIAGNÓSTICAS.

1.5.1 Cuadro No. 1. Matriz de relación diagnóstica.

OBJETIVO	VARIABLE	INDICADOR	FUENTE DE INFORMACIÓN	TÉCNICA
Verificar una adecuada estructura orgánica funcional de la Unidad de Riesgos dentro de la institución.	Estructura orgánica funcional	Estructura Orgánica, Funciones Perfiles	Primaria	Entrevista
Analizar los procesos con los que cuenta la institución para el desarrollo de sus operaciones diarias.	Levantamiento de Procesos	Gobernantes Productivos Habilitantes	Primaria	Entrevista
Evaluar la gestión de riesgo operativo efectuada por las diferentes áreas de la institución las cuales son las encargadas de su control y seguimiento.	Gestión de riesgos.	Fallas en Procesos Fallas de Personas Fallas de Tecnología de la información Fallas por Eventos externos Continuidad del Negocio Procesos Provistos por Terceros	Primaria	Entrevista Encuesta
Determinar la calidad del talento humano con el que cuenta la institución para el desarrollo de sus operaciones diarias.	Administración de talento humano	Vinculación Permanencia Promoción Motivación Desvinculación	Primaria	Encuesta
Definir las fuentes de exposición de riesgo operativo en base a la información levantada por la institución.	Fuentes de exposición al riesgo	Mecanismos de levantamiento de información implementados Frecuencia de Reportes.	Primaria Secundaria	Entrevista Observación
Determinar el nivel de tecnología con el que cuenta la institución para la medición de Riesgo operativo.	Hardware y software	Sistema implementado Bases de datos de eventos	Primaria	Encuesta
Determinar los controles implementados para la prevención de riesgo operativo.	Controles Implementados	Controles concurrentes y posteriores	Primaria	Encuesta

Fuente directa

Elaborado por: Autor del proyecto

1.6 MECÁNICA OPERATIVA

1.6.1 Identificación de la población.

Debido a que la presente investigación se realiza en la Mutualista Imbabura de la ciudad de Ibarra, la población la constituyen todos los empleados y funcionarios que actualmente laboran en esta institución, es decir Directivos, jefes departamentales, empleados y socios en general; se utilizó un CENSO, es decir se aplicó a todo el universo

1.6.2 Cálculo de la muestra.

En el presente proyecto de investigación no se requiere realizar ningún cálculo de la muestra en base al total de la población, ni se emplea fórmula alguna para ello, cabe destacar que se cuenta con el dato exacto de la población: 46 funcionarios, 22 miembros entre representantes de la junta general de asociados y miembros del directorio, dando un total de 68 individuos; en vista de que el tema producto de este documento se refiere a las fallas en: procesos, personas, tecnología de la Información y eventos externos se procederá a involucrar al personal técnico de mayor conocimiento sobre los factores a evaluar de acuerdo a los requerimientos posteriores, así como también a los funcionarios operativos y de soporte.

1.6.3 Información primaria.

Se procedió a utilizar las siguientes formas de recolección de información primaria.

- **Encuesta**, la cual consiste de preguntas principalmente cerradas mediante las cuales se obtiene principalmente información sobre el nivel de conocimiento del personal sobre riesgo operativo.

- **Entrevista**, la cual fue aplicada a las jefaturas departamentales de la institución, y cuyas preguntas están directamente relacionadas con la implementación de riesgo operativo, quienes a su vez se apoyaron en los criterios de sus subalternos.

1.6.4 Información Secundaria.

La información secundaria que se utilizó fue la bibliografía de riesgos, documentos como: las normas internacionales de Basilea, la codificación de resoluciones de la Superintendencia de Bancos y Seguros de Ecuador y documentos relacionados con la linografía para la administración de riesgos en las instituciones financieras.

La información bibliográfica sobre el tema de tesis es bastante limitada.

1.6.5 Diseño de instrumentos investigativos.

Con la finalidad de determinar los instrumentos en la realización de la investigación se desarrolla las encuestas dirigidas al personal operativo o de apoyo y las entrevistas al representante legal, junta de socios, directivos y a las principales jefaturas para medir el grado de exposición a todos los factores de riesgo operativo según la responsabilidad de las áreas y departamentos con los que cuenta la Mutualista Imbabura.

La encuesta anónima y las entrevistas efectuadas al total de la población permiten establecer que en la Mutualista Imbabura no se cuenta con un manual de riesgo operativo.

1.7 EVALUACIÓN DE LA INFORMACIÓN OBTENIDA

Gracias a la aplicación de las entrevistas a los miembros del directorio representante legal y miembros de la junta general de asociados y la

encuesta al personal operativo y de apoyo, de Mutualista Imbabura como principal fuente de recopilación de información se pudo obtener los siguientes resultados:

1.7.1. Entrevista al Jefe de Recursos Humanos

¿La Estructura Orgánica de la institución contempla la unidad de riesgos?

La Mutualista Imbabura desde que se emitió la resolución 631 de riesgos por parte de la Superintendencia de Bancos creó la Unidad Integral de Riesgos quien reporta directamente a la Gerencia General y por intermedio del CAIR (Comité Integral de Riesgos) al Directorio de la institución. Se encuentra constituida por una sola persona quien se encarga de dar cumplimiento a todas sus funciones asignadas.

¿Se ha definido formalmente las funciones asignadas al personal de la Unidad de Riesgos en cuanto a sus obligaciones y responsabilidades?

La Mutualista Imbabura cuenta con un manual de funciones en el que se contempla todas las funciones y responsabilidades del Oficial de Riesgos, estas funciones se encuentran debidamente aprobadas por el Directorio de la institución y se monitorea su cumplimiento por parte de Auditoría Interna dentro de sus evaluaciones.

¿El personal que labora en la Unidad de Riesgos de la institución cumple con los perfiles mínimos requeridos por la instrucción en cuanto a sus actitudes y aptitudes?

Existe un solo empleado a cargo de este departamento, es egresado de la carrera de Contabilidad y Auditoría el cual ha cumplido a cabalidad las

funciones asignadas manteniéndose pendiente la obtención de su título terminal.

¿La institución cuenta con un mapa de procesos en los que los que se haya agrupado de acuerdo al requerimiento de la SBS (Gobernantes, Productivos y Habilitantes)?

El mapa de procesos de la entidad se ha definido a través de los resultados obtenidos por la consultoría contratada con la Empresa Líderes.

¿Se han levantado los procesos identificados en la entidad?

Se encuentra en trámite el levantamiento de los procesos de la institución esto también se lo ha venido desarrollando bajo el asesoramiento de la empresa líderes.

¿La institución cuenta con un manual de administración del Recursos Humano?

Si se cuenta con un manual para la administración del recurso humano el mismo que ha sido aprobado por el Directorio de la Institución así como un reglamento interno de trabajo que se encuentra actualizado al mes de abril del 2011.

¿En este manual se estipulan las políticas de Vinculación, permanencia, motivación, promoción y desvinculación del personal?

El manual únicamente contaba con políticas de vinculación y permanencia en la institución del recurso humano pero actualmente se están desarrollando las políticas de motivación, promoción y desvinculación, mismas que una vez que sean concluidas serán sometidas a revisión y

aprobación del Directorio de la institución y a su difusión interna para su implementación inmediata en beneficio del personal.

¿Se encuentran definidas las políticas de capacitación permanente al personal?

Todos los años dentro del presupuesto institucional se destina un rubro para capacitaciones por área dando preferencia principalmente al personal operativo, la política como tal no ha sido definida dentro del manual de talento humano de la institución ni tampoco se ha considerado la opción al mediano plazo de incluirla.

De las respuestas obtenidas se puede concluir que a pesar de que existe un grado amplio de implementación de los temas de riesgo operativo asociados con el manejo de talento humano aún existen aspectos que se deberán concluir para lograr una implementación adecuada.

FODA de la Entrevista al Jefe de Recursos Humanos

FORTALEZAS		OPORTUNIDADES	
F1	Cuenta con una Unidad de Riesgos debidamente estructurada	O1	Crear una plaza de trabajo adicional para cubrir requerimiento mínimo de personal.
F2	Se encuentran debidamente definidas las funciones y responsabilidades de la unidad de riesgos		
F3	Tienen levantados los manuales de políticas de talento humano		
DEBILIDADES		AMENAZAS	
D1	Existe una sola persona laborando en la Unidad de Riesgos.	A1	Ser sujetos de sanciones, multas u observaciones por parte del organismo de control.
D2	No tiene levantado los procesos en su totalidad.	A2	Incumplir con disposiciones normativas por desconocimiento.
D3	Falta de capacitación específica en temas relacionados a riesgos.		

1.7.2. Entrevista al Auditor Interno.

¿Dentro del Plan Anual de Evaluaciones de su área se contempla revisiones relacionadas al cumplimiento de riesgo operativo?

La norma de administración de riesgos prevé el control que el auditor interno de forma constante y dentro del plan anual de auditoría se realizan revisiones trimestrales de la implementación de riesgo operativo y de otros riesgos.

¿Con que frecuencia se realizan las supervisiones a la Unidad de Riesgos?

La revisión a la unidad de riesgos es realizada de manera trimestral en cuanto al grado de cumplimiento de los cronogramas establecidos principalmente de riesgo operativo, sería factible realizar controles más frecuentes, pudiendo ser de forma mensual pero la falta del recurso humano en el área de auditoría lo limita el control constante.

¿Cuáles son los temas dentro de riesgo operativo que se revisan en las supervisiones realizadas?

Se revisa lo que se requiere mediante la resolución de la Superintendencia de Bancos y Seguros 834 de riesgo operativo los temas asociados a procesos, personas, tecnología y eventos externos, es decir se realiza una revisión integral y se evalúa su grado de avance.

¿Qué criterio mantiene sobre el cumplimiento de la implementación de riesgo operativo a nivel general?

En realidad se ha podido notar que existe mucha demora en la implementación de riesgo operativo porque trata de un tema bastante extenso y que por su complejidad dificulta llegar a un cumplimiento

adecuado, inclusive por parte de la misma Superintendencia de Bancos se ha venido aplazando su culminación e implementación en varias ocasiones, además se debe a que el recurso humano de riesgos es insuficiente.

¿Qué criterio mantiene sobre el nivel de conocimiento sobre riesgo operativo del personal de la Unidad de Riesgo de la Institución?

El Oficial de Riesgos está bien capacitado sobre el tema, la Gerencia General se ha preocupado por dotarle de las herramientas y la capacitación necesaria para poder cumplir con lo que requiere la norma en cuanto a riesgo operativo.

¿Considera apropiado el aporte de recursos de la Alta Gerencia en la implementación de riesgo operativo?

Existe por parte de la gerencia un comprometimiento total sobre el tema y la inversión que se ha realizado en la institución es considerable, se ha dotado de una herramienta informática adquirida a la empresa Grupo Context para la administración de riesgo operativo, en seguridades tecnológicas y plan de contingencia de sistemas de igual forma, inclusive en cuanto al levantamiento de procesos lo está realizando mediante una consultoría con la empresa Lideres.

¿Según su criterio considera apropiado el grado de exposición de riesgo operativo en la institución?

No es apropiado puesto que no se ha procedido a cuantificar una exposición real ya que existen muchos eventos los cuales no son controlados por falta de políticas específicas para la medición de riesgo operativo que ayuden a mitigar dichos eventos que ocasionan pérdida a la mutualista;

De esta entrevista se pueden destacar que a criterio del auditor interno existe mucha demora en la implementación de riesgo operativo por varios factores entre los más importantes se puede mencionar a la falta de recurso humano en riesgos así como también la falta de políticas definidas para la gestión de riesgos operativos en la institución

FODA de la Entrevista al Auditor interno.

FORTALEZAS		OPORTUNIDADES	
F1	Revisión continua de la implementación de la resolución de Riesgo Operativo.	O1	Adecuada oferta de cursos y capacitaciones en temas de riesgo operativo
F2	Cuenta con una herramienta informática para administrar riesgo operativo	O2	
DEBILIDADES		AMENAZAS	
D1	Demora en la implementación de la resolución de riesgo operativo.	A1	Disposiciones del organismo de control demasiado extensos que dificultan el cumplimiento.
D2	Falta de políticas específicas para la administración de riesgo operativo	A2	

1.7.3. Entrevista al Jefe de Sistemas.

¿En el área de sistemas se ha desarrollado un plan de contingencia que asegure la continuidad del uso del software informático?

El departamento de sistemas cuenta con un plan de contingencia que le permite continuar con las operaciones gracias que se mantiene un servidor se respaldos fuera de la matriz como contingencia esto asegura que máximo en el lapso de una hora se reinicien las operaciones y se pueda continuar con la operatividad normal ya que inclusive se usa un canal de comunicación alternativo. Se han realizado las pruebas necesarias para garantizar el proceso de recuperación y de continuidad

¿Se cuenta con un manual de tecnología de información en donde se contemplen políticas relacionadas a riesgo operativo?

Se cuenta con un manual integral de sistemas debidamente aprobado por el directorio de la institución en donde se está contemplando las principales políticas en cuanto al cumplimiento normativo de la resolución 834 de riesgo operativo de la Superintendencia de Bancos. Estas políticas han sido revisadas por el mismo organismo de control.

¿Cuenta con herramientas informáticas para la administración de riesgo operativo?

Las herramientas informáticas de riesgos están bajo la administración de la unidad de riesgos, se cuenta con un software que se encuentra en proceso de parametrización, el departamento de sistemas se ha encargado de la instalación del sistema pero nada tiene que ver con el uso y administración del mismo.

¿El sistema informático con el que opera la institución contiene un módulo de seguridad que permita controlar los accesos y la asignación de usuarios con sus respectivos roles?

El sistema operativo se denomina Orión del cual la Mutualista adquirió sus códigos fuentes y le ha permitido hacer una serie de incorporaciones y mejoras, cuenta con un módulo de seguridad el cual es administrado por auditoría interna con respecto a la asignación de claves y actividades asociadas a cada uno de los cargos, la administración de los accesos no está a cargo del personal del departamento de sistemas. El sistema en general ha sido validado por una auditoría informática de la Superintendencia de Bancos de la cual no existen observaciones sobre el módulo de seguridades.

¿El cumplimiento normativo de los requerimientos de TI dispuestos por la Superintendencia de bancos es adecuado?

El departamento de sistemas cuenta con un excelente nivel de cumplimiento en cuanto a lo dispuesto por la Superintendencia de Bancos y Seguros en referencia a tecnología de información de riesgo operativo, las actividades cumplidas así como las pendientes han sido notificadas al organismo de control por intermedio del oficial de riesgos de la entidad, se ha dado cumplimiento estricto a lo dispuesto en los cronogramas fijados previamente y no se ha tenido observaciones por parte de la auditora interna por incumplimiento.

El departamento de sistemas de la entidad mantiene el cumplimiento normativo más alto en lo que respecta a tecnología de información requerido por el ente de control. Se ha logrado un alto nivel de cumplimiento debido a que se ha realizado una auditoría que entre otras cosas ha revisado todos los temas de riesgo operativo asociados a TI.

FODA de la Entrevista al Jefe de Sistemas.

FORTALEZAS		OPORTUNIDADES	
F1	Cuenta con un plan de contingencia que le permite continuar con las operaciones gracias que se mantiene un servidor se respaldos fuera de la matriz		
F2	Tiene definida las politicas de TI mediante un manual del area		
F3	Sistema con modulo de seguridad administrado por Auditora Interna		
DEBILIDADES		AMENAZAS	
		A1	Exposición a sanciones por parte del organismo de control por incumplimiento normativo

1.7.4. Entrevista al Directorio, Representantes y Gerencia General.

¿Cuál ha sido el aporte de la administración en la implementación de riesgo operativo dentro de la institución?

El Directorio a aprobado un valor considerable en inversión para la implementación de riesgo operativo tanto para el área de riesgos como para las demás áreas, lo cual está facilitando la implementación de todo lo que se requiere en este tema

¿Existe la apertura por parte de la administración para la capacitación del personal de la unidad de Riesgos en temas relacionados a riesgo operativo?

Si existe esa apertura por parte del Directorio y la Gerencia, sabiendo de la importancia del tema para la institución. Principalmente a la Unidad de Riesgos se le ha capacitado en temas afines a su cargo con la finalidad de que sean difundidos los conocimientos adquiridos a las demás reas de la institución.

¿La Junta General de Asociados ha dictado algún tipo de disposición para agilizar la implementación de riesgo operativo en la institución?

La Junta General de Asociados no se ha pronunciado sobre este tema, a pesar de que en las reuniones de la junta se presentan informes por áreas existe una total desinformación sobre riesgo operativo, se desconoce inclusive los beneficios que esto podría ocasionar a los socios de la entidad y al personal en general.

¿Considera usted necesario la dotación de personal para fortalecer la Unidad de Riesgos de la Institución?

Se contempla en un futuro el fortalecimiento de esta área pero por el momento no está considerado en el presupuesto, se ha dado preferencia a contratar personal en áreas comerciales.

¿La gerencia General o el Directorio realizan algún tipo de seguimiento a la implementación de Riesgo Operativo realizado principalmente por el Oficial de Riesgos?

En las reuniones de directorio se analizan y aprueban las actas del Comité de Administración Integral de Riesgos en el cual ente otras cosas se trata un punto específico sobre este tema, al igual que se analizan y aprueban los informes de Auditoría Interna en el que se da seguimiento a la implementación de riesgo operativo o de ser necesario se solicitan informes específicos sobre el tema al Oficial de Riesgos

¿Cómo considera la implementación de Riesgo operativo dentro de la Institución?

Se ha logrado avanzar en muchas cosas principalmente a temas tecnológicos, pero aún no existe un manual específico de riesgo operativo en el que definan todas las políticas y procedimientos de administración de riesgo operativo de acuerdo a lo que señala la normativa del organismo de control. Esto hace que se mantenga una alta exposición a eventos de pérdida sin que existan los controles establecidos para prevención y mitigamiento de dichos eventos que a la final le cuestan a la institución.

De las respuestas emitidas por el personal entrevistado se evidencia un desconocimiento generalizado sobre la necesidad de gestionar riesgo

operativo en la institución la cual ha dado preferencia a la contratación de personal para fortalecer el área comercial y no ha contemplado la contratación de personal técnico de riesgos. Los representantes de la institución desconocen de los principales beneficios que se podrían generar para los socios al controlar riesgo operativo.

FODA de la Entrevista al Directorio, Representantes y Gerencia General

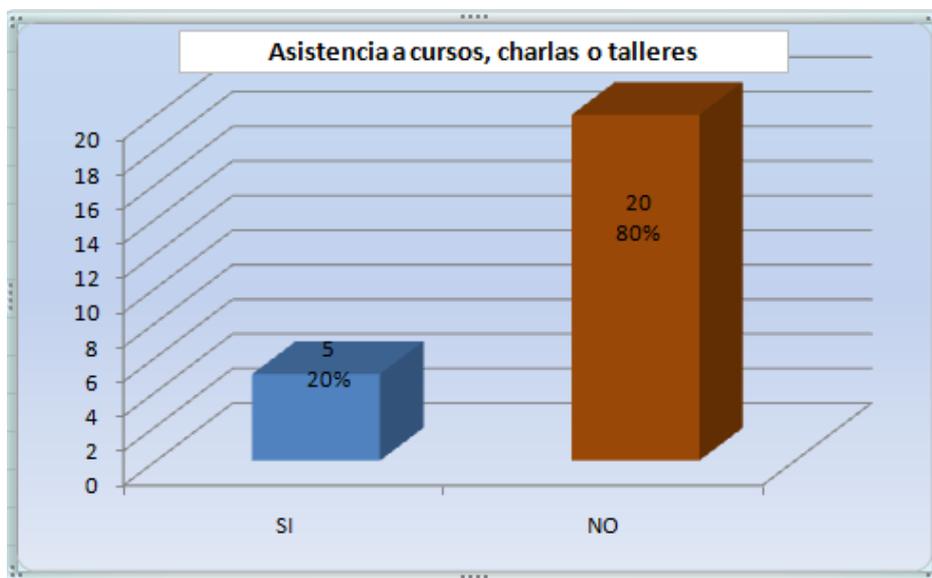
FORTALEZAS		OPORTUNIDADES	
F1	Administración comprometida con la implementación de riesgo operativo	O1	Crear una plaza de trabajo adicional para cubrir requerimiento mínimo de personal.
F2	Compromiso de la administración en cuanto a capacitación se refiere		
DEBILIDADES		AMENAZAS	
D1	Justa General de asociados no ha dictado disposiciones o requerimientos sobre riesgo operativo	A1	Posibles sanciones por incumplimiento normativo de resolución de riesgo operativo.
D2	Personal insuficiente para la Unidad de riesgos		
D3	Seguimiento realizado unidamanete por intermedio de las actas de Comité de Riesgos		
D4	No existe Un manual específico de Riesgo Operativo		

1.7.5. Encuesta dirigida al personal operativo y de soporte.

1. ¿Ha asistido a cursos, charlas o talleres relacionados a riesgo operativo en el transcurso de su vida profesional?

SI	NO	
5	20	Encuestados
20	80	Porcentaje

Grafico No. 1. ASISTENCIA A SEMINARIOS.



Fuente: Resultados de la encuesta

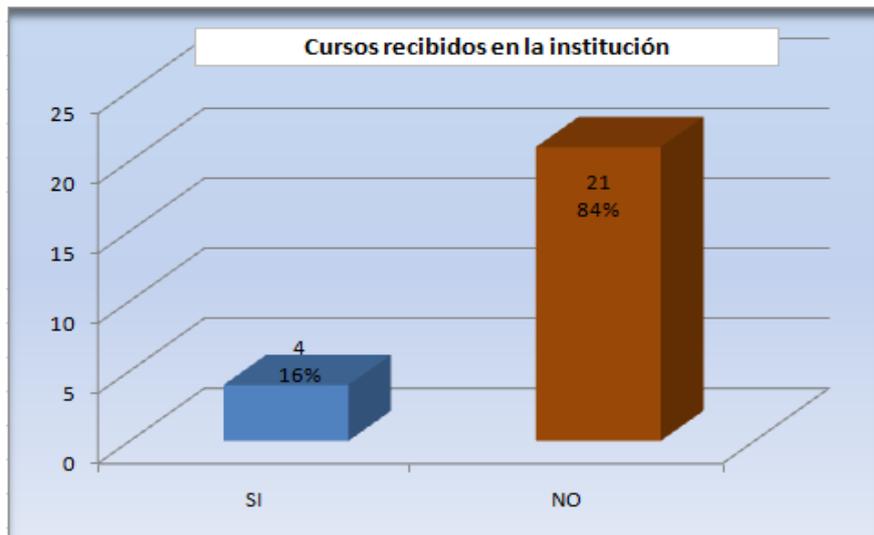
Elaboración: Autor del proyecto

Del talento humano encuestado un bajo porcentaje se ha capacitado en administración de riesgos operativos en el transcurso de su vida profesional, evidenciando un débil conocimiento del personal en cómo identificar, medir, controlar/monitorear y mitigación los riesgos a los que se ve expuesta la institución. El desconocimiento del personal también expone al personal de la institución a incurrir en eventos que podrían ocasionar pérdida para la institución

2. ¿En esta institución ha recibido algún curso relacionado con riesgo operativo?

SI	NO	
4	21	Encuestados
16	84	Porcentaje

Grafico No. 2 CAPACITACIÓN RECIBIDA EN LA INSTITUCIÓN.



Fuente: Resultados de la encuesta

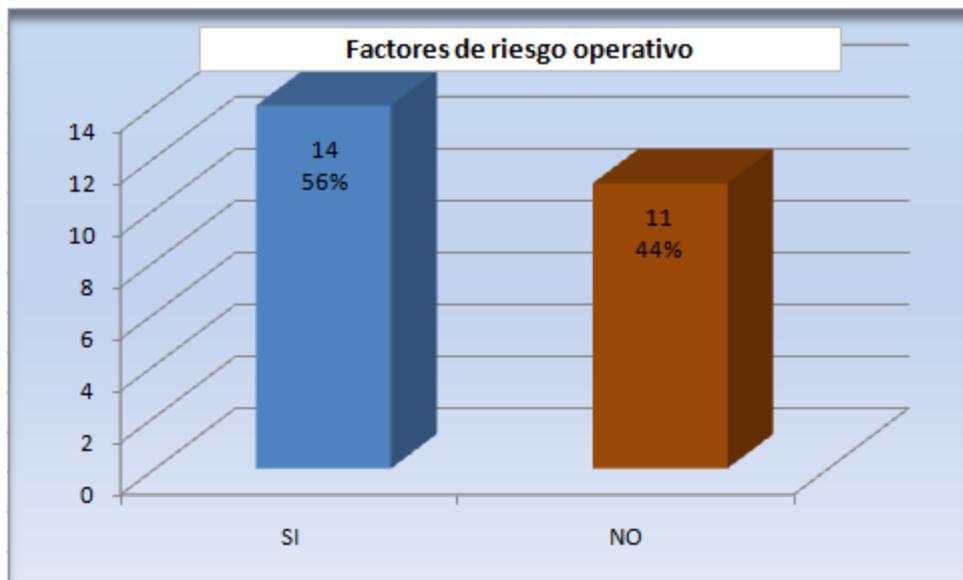
Elaboración: Autor del proyecto

Existe un plan de capacitación en talento humano en el cual no se contempla capacitar al personal en temas relacionados con riesgo operativo, un muy bajo número de funcionarios ha sido capacitado en riesgos dejando en evidencia la falta de preocupación de la administración de la institución en capacitar a su personal sobre este tema. El personal de riesgos es el único que se le ha dado una capacitación completa sobre el tema, pero la falta de conocimiento de los demás funcionarios expone a la institución a una mayor exposición al riesgo.

3. ¿Conoce usted cuales se denominan como factores de riesgo operativo?

SI	NO	
14	11	Encuestados
56	44	Porcentaje

Grafico No. 3 FACTORES DE RIESGO OPERATIVO.



Fuente: Resultados de la encuesta

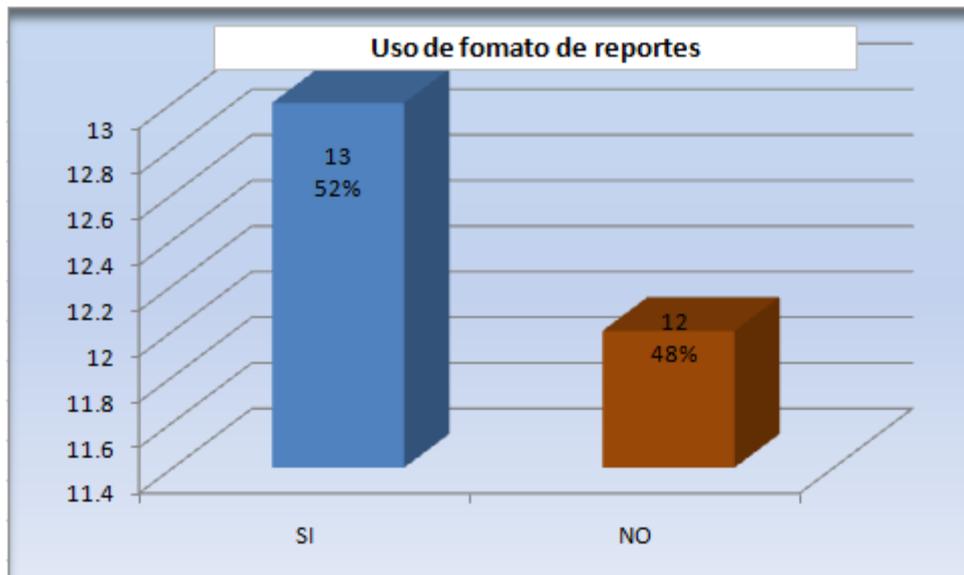
Elaboración: Autor del proyecto

Los conocimientos del personal sobre riesgos se lo ha fortalecido por la difusión interna de la unidad de riesgos, lo cual guarda relación con las respuestas anteriores, los informes de auditor interno no han incluido recomendaciones para fortalecer el conocimiento de riesgos del personal de la institución y de esta manera prevenir el impacto que se podría generar. Más del 50% de los encuestados conocen únicamente sobre temas básicos de riesgo operativo

4. ¿Ha utilizado el formato de reportes de eventos de riesgo operativo implantado por la Unidad de Riesgos de la Institución?

SI	NO	
13	12	Encuestados
52	48	Porcentaje

Grafico No. 4 USO DEL FORMATO DE REPORTES DE EVENTOS DE RIESGO OPERATIVO.



Fuente: Resultados de la encuesta

Elaboración: Autor del proyecto

El reporte de riesgo operativo es un formato que deben enviar todos los funcionarios a la unidad de riesgos haciendo conocer las fallas o errores cometidos en procesos, o por personas, tecnología de información, así como los eventos externos en sus actividades diarias, aproximadamente la mitad de los funcionarios utilizan este mecanismo de reporte para que el responsable de esta unidad alimente la base de eventos, un alto porcentaje de empleados no utilizan este reporte a pesar de que existe la disposición de la administración para hacerlo.

5. ¿Cuáles son las causas por las que Usted se debería limitado a no reportar los errores cometidos dentro de su puesto de trabajo?

Encuestados	Porcentaje
6	24
6	24
4	16
9	36
0	0
25	100%

Grafico No. 5. CAUSAS POR LAS QUE NO REPORTARÍA ERRORES.



Fuente: Resultados de la encuesta

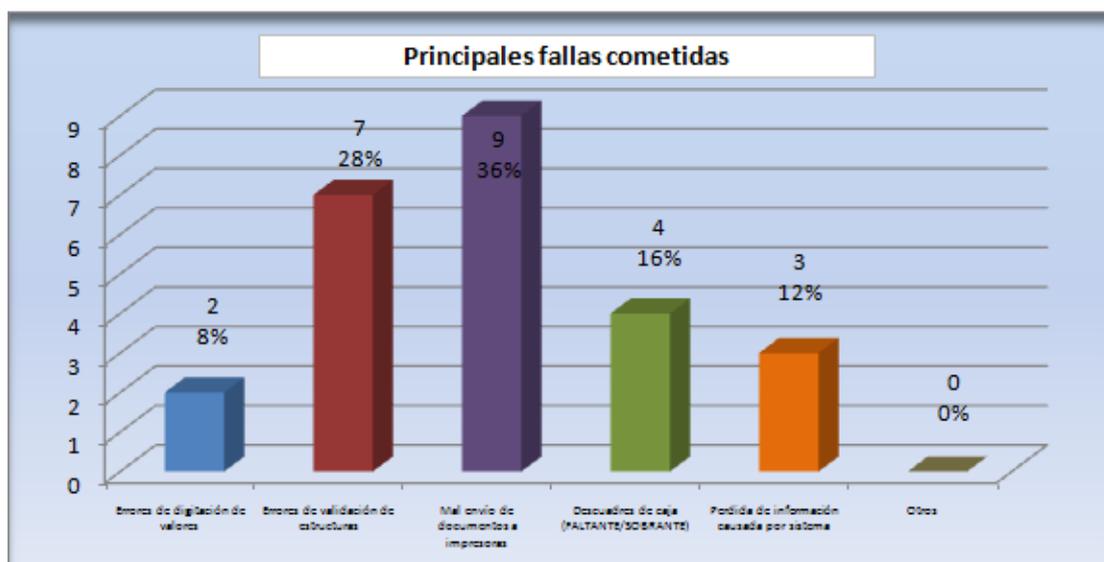
Elaboración: Autor del proyecto

La mayor parte del talento humano de la institución manifiesta el temor a usar este mecanismo de reporte por no exponerse a llamados de atención, sanciones económicas o inclusive llegar a perder el empleo por los errores cometidos, un menor porcentaje de los encuestados afirma utilizar el mecanismo de reportes en todos los eventos cometidos. Al ser la mayor parte del personal quienes no reportan los errores cometidos, existe una deficiencia de información considerable para poder procesar la base de eventos ya que no se podría cuantificar un valor real de pérdida esperada.

6. ¿Cuáles son sus principales fallas al momento de realizar las actividades para las que fue contratado en la institución?

Encuestados	Porcentaje
2	8
7	28
9	36
4	16
3	12
0	0
25	100%

Grafico No. 6 PRINCIPALES FALLAS AL MOMENTO DE REALIZAR SUS ACTIVIDADES.



Fuente: Resultados de la encuesta

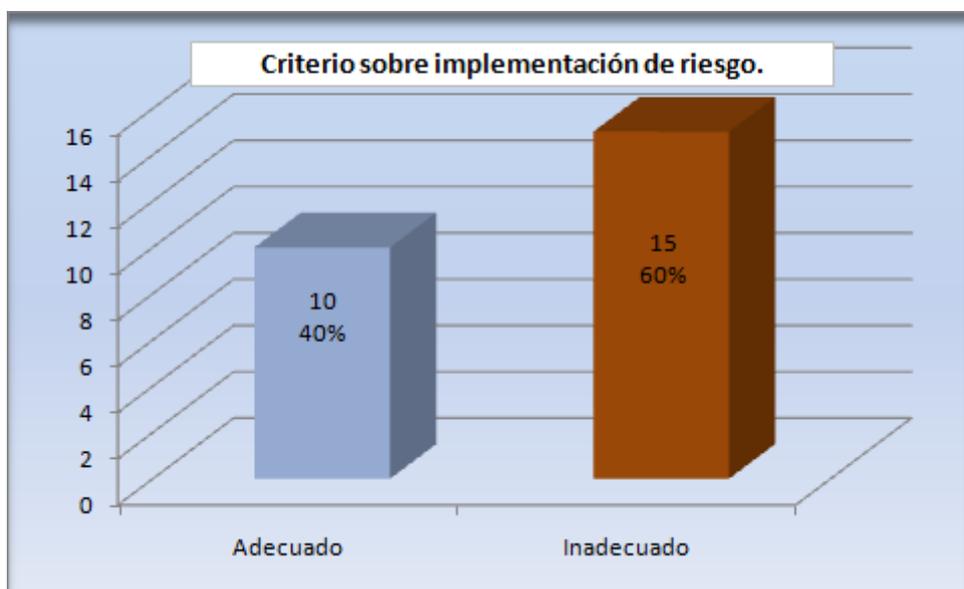
Elaboración: Autor del proyecto

De todo el universo de eventos de riesgos se seleccionaron los que a criterio del personal de riesgos son los más frecuentes asociados a fallas de personas siendo a pesar de que la severidad es baja el nivel de frecuencia reportado es alto y al no ser controlados de manera adecuada ocasionan una pérdida considerable de recursos en la institución

7. Emita su criterio sobre la implementación de Riesgo operativo en la Institución.

Adecuado	Inadecuado	
10	15	Encuestados
40	60	Porcentaje

Grafico No. 7 CRITERIO SOBRE LA IMPLEMENTACIÓN DE RIESGO OPERATIVO EN LA INSTITUCIÓN.



Fuente: Resultados de la encuesta

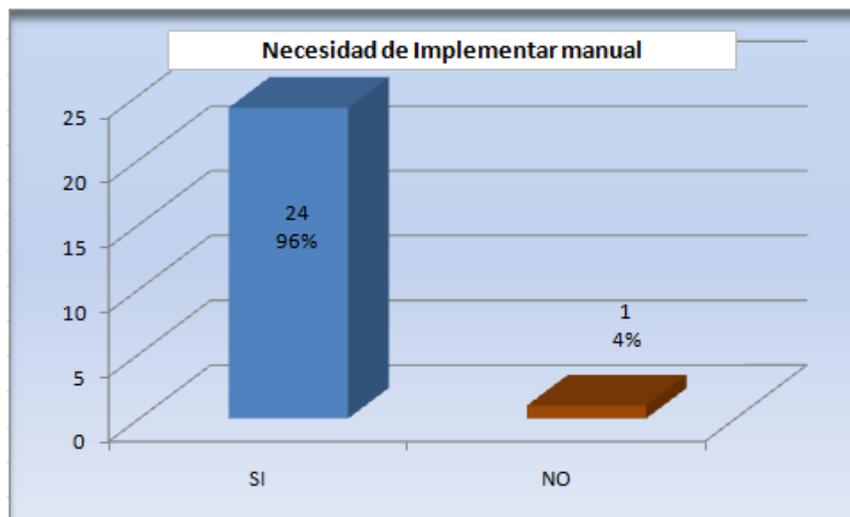
Elaboración: Autor del proyecto

La implementación de riesgo operativo es una necesidad de la institución la cual no se la ha realizado de manera correcta debido a la falta de compromiso del personal de la institución tanto para reportar los eventos detectados como para generar una cultura organizacional para la administración de riesgo. Un alto porcentaje del personal encuestado considera inadecuado el proceso de implementación de riesgo operativo.

8. ¿Considera necesaria la implementación de un manual de riesgo operativo en la institución?

SI	NO	
24	1	Encuestados
96	4	Porcentaje

Grafico No. 8 CONSIDERA NECESARIO LA IMPLEMENTACIÓN DE UN MANUAL DE RIESGOS.



Fuente: Resultados de la encuesta

Elaboración: Autor del proyecto

Por último se consultó a todos los encuestados si consideran necesaria la implementación de un manual de riesgo operativo en la institución en un solo caso la respuesta fue negativa dejando en evidencia que la falta de una normativa institucional de administración de riesgo operativo está ocasionando un perjuicio a la entidad. Auditoría interna no se ha pronunciado oficialmente sobre una evaluación integral al proceso de implementación en donde deje en evidencia las falencias detectadas.

1.8 CONSTRUCCIÓN DE LA MATRIZ FODA.

Cuadro No. 2. Matriz FODA.

FORTALEZAS		OPORTUNIDADES	
F1	Alto grado de implementación de la normativa actual de Riesgos	O1	Control y supervisión constante de parte de la Superintendencia de bancos que aporta en la minimización de exposición al riesgo
F2	Toma decisiones en base a las políticas dictadas por el organismo de control o internamente en la institución	O2	Supervisión personalizada por parte de funcionarios capacitados del ente de control
F3	Personal con experiencia responsable y comprometido con la institución	O3	Stock de herramientas informáticas para la administración de riesgos en caso de que el proveedor incumpla con el contrato
F4	Dotación de infraestructura informática para la Unidad de riesgos	O4	Cursos de capacitación frecuentes con relación a riesgo operativo
F5	Capacitación interna constante	O5	Incrementar el número de clientes por mejoras en procesos comerciales
F6	Infraestructura adecuada para el desarrollo de sus actividades		
DEBILIDADES		AMENAZAS	
D1	No cuenta con una base de eventos de riesgos operativo adecuada para determinar Severidad y Frecuencia	A1	Falta de profesionales en el medio con conocimiento y experiencia en riesgos
D2	Saturación de actividades del personal del área de riesgos	A2	Insuficiente material bibliográfico para soporte técnico en la administración de riesgo operativo
D3	No se difunde adecuadamente al personal los procesos de la institución	A3	Perdida de clientes que prefieren otras instituciones financieras por tiempos de respuesta demasiado largos asociado a inadecuados procesos
D4	Rotación de personal en áreas críticas	A4	Factores externos que interrumpan las actividades normales de la institución
D5	Limitado personal en el área de riesgos	A5	Comentarios maliciosos por parte de clientes insatisfechos que ocasionen riesgo reputacional
D6	Temor del personal a reportar Riesgo operativo para evitar sanciones y llamados de atención	A6	Control in situ demasiado prolongado por parte de la SBS que absorbe el tiempo del personal clave de la institución (jefes departamentales)
D7	No se mantiene Registros formales de eventos de riesgo operativo detectados en el Departamento de sistemas		
D8	Falta de políticas de prevención de Riesgos en diferentes áreas		

Fuente: Resultados de la encuesta

Elaboración: Autor del proyecto

1.9 EVALUACIÓN DE INFORMACIÓN ESTRATÉGICA FA, FO, DO, DA.

Cuadro No. 3. CRUCES ESTRATÉGICOS.

		OPORTUNIDADES		AMENAZAS	
		O1	O2	A1	A2
MATRIZ DE CRUCES ESTRATÉGICOS (FO - FA - DO - DA)		Control y supervisión constante de parte de la Superintendencia de bancos que aporta en la minimización de exposición al riesgo	Supervisión personalizada por parte de funcionarios capacitados del ente de control	Falta de profesionales en el medio con conocimiento y experiencia en riesgos	Insuficiente material bibliográfico para soporte técnico en la administración de riesgo operativo
		Stock de herramientas informáticas para la administración de riesgos en caso de que el proveedor incumpla con el contrato	Cursos de capacitación frecuentes con relación a riesgo operativo	Perdida de clientes que prefieren otras instituciones financieras por tiempos de respuesta demasiado largos asociado a inadecuados procesos	Factores externos que interrumpan las actividades normales de la institución
		Incrementar el número de clientes por mejoras en procesos comerciales		Comentarios maliciosos por parte de clientes insatisfechos que ocasionen riesgo reputacional	Control in situ demasiado prolongado por parte de la SBS que absorbe el tiempo del personal clave de la institución (jefes departamentales)
FORTALEZAS		FO		FA	
F1	Alto grado de implementación de la normativa actual de Riesgos	Aprovechando la supervisión del personal de la SBS poder cumplir con la implementación de riesgo operativo con su revisión y acompañamiento		Contando con un plan de continuidad de Negocio que permita enlistar una serie de pasos a seguir por parte del personal en caso de interrupción de las actividades por factores externos.	
F2	Toma decisiones en base a las políticas dictadas por el organismo de control o internamente en la institución	Implementando las políticas de riesgo operativo en base a las normativas vigentes de parte del organismo de control		Mejorando la imagen institucional para fortalecer su posicionamiento evitando impactos graves por comentarios maliciosos que afecten su reputación.	
F3	Personal con experiencia responsable y comprometido con la institución	Capacitando al personal no solo de la unidad de Riesgos sino a todas las jefaturas sobre temas relacionados a la medición de Riesgo operativo		Determinando políticas de acuerdo a la realidad de la institución basadas en resultados debido a la dificultad de encontrar fuentes bibliográficas que sirvan de guía	
F4	Dotación de infraestructura informática para la Unidad de riesgos	Determinando proveedores alternos para obtener el servicio informático para administrar riesgo operativo		Coordinando las visitas de parte de la SBS y el personal de la institución para evitar pérdidas de tiempo por encontrarse justificando los requerimientos del ente de control	
F5	Capacitación interna constante	Contando con la infraestructura adecuada para la incrementación de clientes por mejoras en procesos que permitan agilizar la atención minimizando la exposición al riesgo			
F6	Infraestructura adecuada para el desarrollo de sus actividades				
DEBILIDADES		DO		DA	
D1	No cuenta con una base de eventos de riesgos operativo adecuada para determinar Severidad y Frecuencia	Implementando mejores alternativas de recolección de datos para alimentar la base de eventos de pérdida por exposición a riesgo operativo		Educando al personal responsable de la realización de reportes constantes de los eventos detectados, insistiendo en la necesidad institucional de cuantificar la pérdida por exposición a riesgo operativo	
D2	Saturación de actividades del personal del área de riesgos	Mejorando los canales de comunicación mediante la implementación de una intranet que permita que todo el personal tenga acceso a revisar los procesos institucionales		Dotando a la Unidad de Riesgos del Recurso Humano necesario a nivel de asistentes para mejorar la ejecución de las actividades pendientes	
D3	No se difunde adecuadamente al personal los procesos de la institución	Capacitando y motivando al personal para evitar la rotación actual especialmente en las áreas críticas de la institución.		Formando al personal de riesgos y fortaleciendo sus capacidades mediante la capacitación integral en temas relacionados con riesgo operativo.	
D4	Rotación de personal en áreas críticas	Mejorando el sistema de reportaría del área de sistemas para mantener una base de eventos asociada a fallas en software y hardware		Dotando al área de sistemas de una infraestructura adecuada que permitan un servicio constante luego de la exposición a un evento de riesgo que amenace con interrumpir las actividades institucionales.	
D5	Limitado personal en el área de riesgos	Capacitando al personal de riesgos para que se definan las políticas de prevención de riesgos a nivel de toda la institución			
D6	Temor del personal a reportar Riesgo operativo para evitar sanciones y llamados de atención				
D7	No se mantiene Registros formales de eventos de riesgo operativo detectados en el Departamento de sistemas				
D8	Falta de políticas de prevención de Riesgos en diferentes áreas				

Fuente: Resultados de la encuesta

Elaboración: Autor del proyecto

1.10 IDENTIFICACIÓN DE PROBLEMAS EN RELACIÓN CAUSA EFECTO.

Concluida la investigación de campo en las que se aplicó las respectivas técnicas de recopilación de información, tanto encuentra como entrevista, se logró obtener información relevante, con la cual podemos determinar la necesidad de Mutualista Imbabura de Contar con “Un Manual de Riesgo Operativo” que permita identificar, medir, controlar / mitigar y monitorear la exposición al riesgo operativo de la institución, problema que puede ser explicado por las siguientes causas con sus respectivos efectos:

- Se evidencia una inadecuada estandarización de los procesos con los que cuenta la institución, mismos que actualmente están siendo levantados por una empresa consultora. Al no existir una estandarización de los procesos existe una desorganización en la realización de las actividades del personal.
- No se cuenta con políticas de control para administrar riesgo operativo por parte de la unidad integral de riesgos. Al no existir políticas de control el seguimiento y evaluación de su cumplimiento se ve limitado y se expone a la entidad a posibles pérdidas por falta de control
- No se cuenta con una metodología definida para medir, controlar y monitorear los riesgos operativos identificados. Lo cual no permite cuantificar con certeza las cifras exactas de las pérdidas esperadas por la exposición al riesgo operativo que se genera dentro de la institución
- No se ha definido un formato estandarizado de reportes de eventos de riesgo operativo. Por tal razón existe un incumplimiento generalizado del personal sobre los reportes que se deben realizar

a la unidad de riesgos para notificar e informar los errores cometidos.

- Inadecuada delimitación de funciones del personal de la Unidad de Riesgos quien manifiesta no contar con el tiempo necesario para poder implementar riesgo operativo en la institución. Ocasiona incumplimientos en el desarrollo de la implementación de riesgo operativo, tema que requiere de total dedicación para su implementación.
- Se encuentra en proceso de implementación una herramienta de administración de riesgo operativo en la cual a un no se ha definido la metodología de cuantificación de severidad y frecuencia de los eventos detectados. Administrar de manera ordenada riesgo operativo contando con mecanismos de reportería que

Por lo expuesto anteriormente considero oportuno elaborar e implementar el **“MANUAL DE RIESGO OPERATIVO PARA MUTUALISTA IMBABURA”**.

CAPÍTULO II

2. MARCO TEÓRICO

2.1 ENTIDADES FINANCIERAS.

La Ley General de Instituciones del Sistema Financiero en el artículo 2 señala:

Artículo 2 “Se caracterizan principalmente por ser intermediarios en el mercado financiero, en el cual actúan de manera habitual, captando recursos del público para obtener fondos a través de depósitos o cualquier otra forma de captación, con el objeto de utilizar los recursos así obtenidos, total o parcialmente, en operaciones de crédito e inversión”.
Pago. 3

Las entidades financieras son el principal motor de la economía nacional que permite por medio del crédito, la inversión y la captación de fondos a la vista y a plazo como principales productos la generación de recursos monetarios para el desarrollo económico local regional y nacional.

2.2 TIPOS DE ENTIDADES FINANCIERAS

Artículo 2 de la LEY GENERAL DE INSTITUCIONES DEL SISTEMA FINANCIERO “son instituciones financieras privadas los bancos, las sociedades financieras o corporaciones de inversión y desarrollo, las asociaciones mutualistas de ahorro y crédito para la vivienda y las cooperativas de ahorro y crédito que realizan intermediación financiera con el público.

Los bancos y las sociedades financieras o corporaciones de inversión y desarrollo”. Pág. 3

2.3 ENTIDADES DE CONTROL DE INSTITUCIONES FINANCIERAS EN EL ECUADOR.

Existen en la actualidad dos tipos de organismo de control para las instituciones financieras nacionales como son la Superintendencia de Bancos y Seguros que se encargan del control y monitoreo de bancos, sociedades financieras y mutualistas de ahorro y crédito principalmente y la actualmente creada Superintendencia de Economía Popular y solidaria que se encarga del monitoreo y control de las cooperativas de ahorro y crédito entre otras funciones.

2.4 DESCRIPCIÓN DE MUTUALISMO.

Según la real academia de la lengua publica en el Diccionario Océano Uno la definición del mutualismo como un “movimiento corporativo destinado a formar sociedades de ayuda mutua” así como también lo define como “asociación entre individuos de distinta especie en que ambas partes resultan beneficiadas”. Edición 2.008, Pág. 1.112

Según lo consultado en el sitio web de la wikipedia se emite la siguiente consideración del mutualismo:

El mutualismo se diferencia de otras interacciones en las que una especie se beneficia a costas de otra; éstos son los casos de explotación.

[http://es.wikipedia.org/wiki/Mutualismo_\(biolog%C3%ADa\)](http://es.wikipedia.org/wiki/Mutualismo_(biolog%C3%ADa))

La naturaleza y objetivo social de estas entidades se revalida en el artículo 2 de la Ley General de Instituciones del Sistema Financiero actualmente en vigencia que establece:

"Las Asociaciones Mutualistas de Ahorro y Crédito para la Vivienda son instituciones cuya actividad principal es la captación de recursos del público para destinarlos al financiamiento de la vivienda, la construcción y el bienestar social de sus asociados, que deberá evidenciarse en la composición de sus activos". Pág. 4

Ley promulgada del 12 de mayo de 1994 y cuyo reglamento fue emitido el 4 de julio del mismo año.

2.4.1 Mutualista Imbabura.

Es una institución financiera debidamente constituida la cual cumplió con todos sus requisitos de creación y fue aprobada por el Banco Ecuatoriano de la Vivienda para su funcionamiento un 19 de noviembre de 1963. Su actividad económica, al igual que la de sus pares difiere de las demás instituciones financieras del Ecuador ya que dentro de sus líneas de negocio contempla también el desarrollo de proyectos inmobiliarios. Los proyectos inmobiliarios de mayor renombre de la institución son los construidos en el sector El Retorno y en la calle Salinas. Dentro de su negocio de intermediación financiera se ha dedicado a la captación de fondos a la vista y a plazo fijo y en crédito coloca todos sus destinos de Consumo, Vivienda, Microcrédito y Comercial.

2.4.2 Organización de Mutualista Imbabura

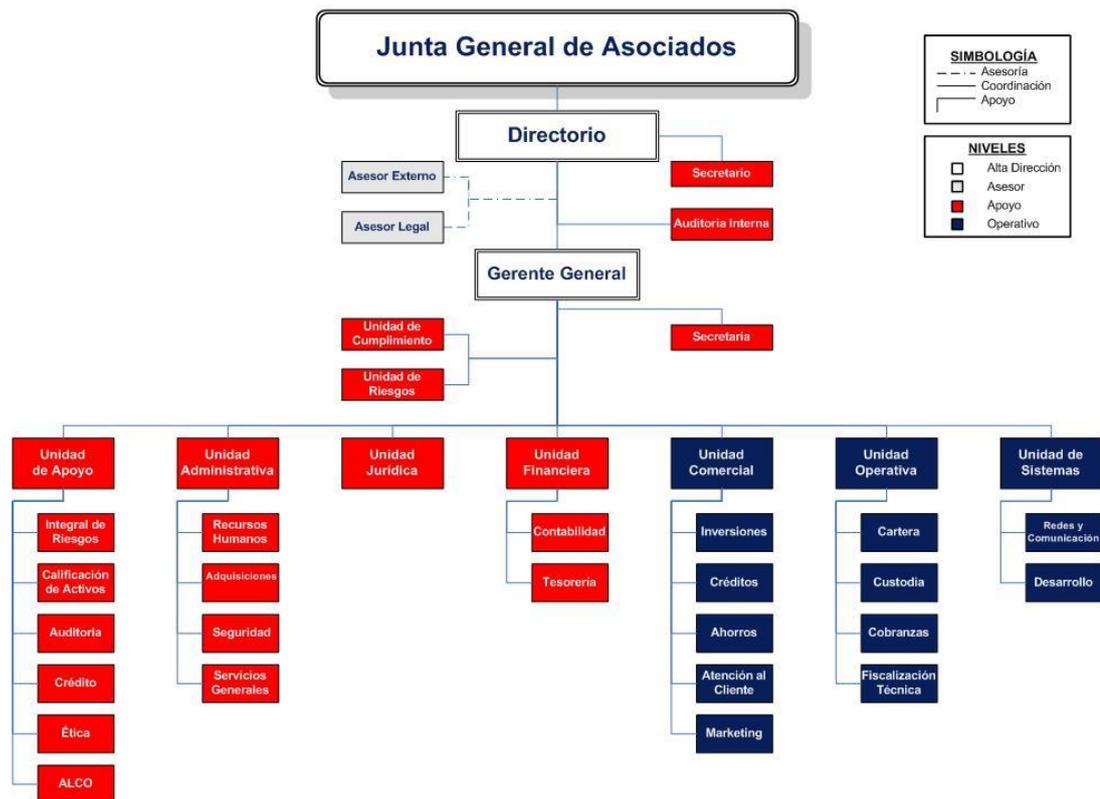
La Mutualista Imbabura cuenta con estructura orgánica subdividida en los siguientes niveles:

- Nivel Gerencial
- Nivel Asesor
- Jefaturas departamentales o de unidad

- Personal de Apoyo.

De acuerdo a lo que señala el Manual de Funciones (actualización al 2010) de la institución su organigrama estructural contempla los siguientes cargos y responsabilidades:

CUADRO No 4. Organigrama de Mutualista Imbabura



Fuente: Manual de Funciones de Mutualista Imbabura

Elaboración: Mutualista Imbabura

2.4.3 Principios del Mutualismo.

Los principios básicos de las mutualidades a nivel general según lo publicado en <https://es.wikipedia.org/wiki/Mutualidad> son los siguientes:

- Adhesión voluntaria.

- Organización democrática
- Neutralidad institucional: política, religiosa, racial y gremial
- Contribución acorde con los servicios a recibir
- Capitalización social de los excedentes
- Educación y capacitación social y mutual
- Integración para el desarrollo.

Información extraída de la reseña histórica de Mutualista Imbabura del 2009.

2.5 RIESGO

2.5.1 Conceptos y definiciones.

A continuación se definen los principales conceptos relacionados con riesgos financieros.

- **Riesgo.-** Es la posibilidad de obtener un resultado adverso en la realización de cualquier actividad.

Según REYES P. En toda actividad y por ende en todo proceso existe la posibilidad de que haya una alteración respecto a sus resultados, se debe entender que existe un riesgo. Así, el riesgo se puede entender como “La variación que se puede producir en los resultados esperados de una situación dada, dentro de un periodo determinado”. Pág. 32, edición 2012.

Según la real academia de la lengua se define riesgo de la siguiente manera: Dicho de acometer una empresa o de celebrar un contrato, Sometiéndose a influjo de suerte o evento, sin poder reclamar por la acción de estos. 22 edición 2010 publicada en el sitio Web <http://lema.rae.es/drae/>.

Y de acuerdo a lo que señala la Norma ASNZ ISO 31000 publicada en el mes de noviembre del 2009 define al término riesgo como El efecto de la incertidumbre en el logro de los objetivos. Esto nos lleva a que el estudio de los riesgos este más enfocado en conocerlos y saber que puede ocurrir tratando de hacer una visualización de futuro y que le permitan a la entidad saber que le depara.

- **Administración de riesgos.** De acuerdo a lo expuesto en la Resolución No. JB-2004-631 de la Superintendencia de Bancos y Seguros del Ecuador La administración de riesgos se define 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”.

2.5.2 Clasificación de los riesgos

2.5.2.1 Riesgo de crédito.

DAQUI R. define el riesgo de crédito como: ***“Es el proveniente de la tenencia de un contrato particular o de un portafolio, como un resultado de que una o más partes relevantes para el contrato (s)***

dejan de cumplir sus obligaciones financieras”. Pág. 74, edición 2.006.

2.5.2.2 Riesgo de mercado.

Las normas internacionales de Basilea conceptualiza al riesgo de mercado como:

“La pérdida potencial por cambios en los factores de riesgo de mercado que inciden sobre la valuación o sobre los resultados esperados de las operaciones activas, pasivas o causantes de pasivo contingente, tales como tasa de interés, tipos de cambio índices de precios, entre otros”.

2.5.2.3 Riesgo de tasa de interés y riesgo de tipo de cambio.

Conceptos incluidos en el LIBRO I DE LAS NORMAS GENERALES PARA LA APLICACIÓN DE LA LEY DE INSTITUCIONES DEL SISTEMA FINANCIERO, mediante resolución JB-2002-429 del 22 de enero del 2002 y reformado mediante resolución No. JB-2003-615 del 23 de diciembre del 2003.

“Es la contingencia de que las instituciones controladas tengo pérdidas como consecuencia de los movimientos de las tasas de interés y cuyo efecto dependerá de la estructura del activo, pasivo y contingente”. Y por tipo de cambio ***“Es el impacto sobre las utilidades y el patrimonio de la institución controlada por variaciones en el tipo de cambio y cuyo impacto dependerá de las posiciones netas que mantenga una institución controlada, en cada una de***

las monedas con las que opera". Pág. 203 de la Codificación de resoluciones de la Superintendencia de Bancos y Seguros del Ecuador.

2.5.2.4 Riesgo de liquidez.

Concepto extraído del LIBRO I DE LAS NORMAS GENERALES PARA LA APLICACIÓN DE LA LEY DE INSTITUCIONES DEL SISTEMA FINANCIERO, mediante resolución JB-2002-431 del 22 de enero del 2002 y reformado mediante resolución No. JB-2003-615 del 23 de diciembre del 2003.

Es la contingencia de pérdida que se manifiesta por la incapacidad de la institución del sistema financiero para enfrentar una escasez de fondos y cumplir sus obligaciones, y que determina la necesidad de conseguir recursos alternativos, o de realizar activos en condiciones desfavorables. Pág. 204 de la Codificación de resoluciones de la Superintendencia de Bancos y Seguros del Ecuador.

2.5.2.5 Riesgo operativo.

De acuerdo a lo expuesto en la Resolución No. JB-2004-631 del 22 de enero del 2004 de la Superintendencia de Bancos y Seguros del Ecuador se define al riesgo operativo como:

Es 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. Pág. 204 de la Codificación de resoluciones de la Superintendencia de Bancos y Seguros del Ecuador.

2.5.2.6 Riesgo legal.

En la Resolución No. JB-2008-1202 del 23 de octubre del 2008 de la Superintendencia de Bancos y Seguros del Ecuador.

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. Pág. 204 de la Codificación de resoluciones de la Superintendencia de Bancos y Seguros del Ecuador.

2.5.2.7 Riesgo de reputación.

En la Resolución No. JB-2004-631 del 22 de enero del 2004 de la Superintendencia de Bancos y Seguros del Ecuador se manifiesta que riesgo reputacional es:

“La posibilidad de afectación del prestigio de una institución del sistema financiero por cualquier evento externo, fallas internas hechas públicas, o al estar involucrada en transacciones o relaciones con negocios ilícitos, que puedan generar pérdidas y ocasionar un deterioro de la situación de la entidad.” Pág. 204

Una vez que se ha procedido a definir cada uno de los riesgos financieros de conformidad con la normativa local e internacional, se desglosa en detalle el contenido de todos los puntos inmersos dentro del tema específico de Riesgo Operativo como tema central de este trabajo de investigación.

2.8 FACTORES DE RIESGO OPERATIVO.

Con el propósito de que se minimice la probabilidad de incurrir en pérdidas financieras atribuibles al riesgo operativo y de acuerdo a lo publicado en la Resolución No. JB-2005-834 de 20 de Octubre del 2005 de la Superintendencia de Bancos y Seguros, deben ser adecuadamente administrados los siguientes aspectos, los cuales se interrelacionan entre sí:

2.8.1 Procesos.

Con el objeto de garantizar la optimización de los recursos y la estandarización de las actividades, las instituciones financieras que se encuentran bajo el control de la superintendencia de bancos y seguros deben contar con procesos definidos de conformidad con la estrategia y las políticas adoptadas por sus directorios u organismo que hagan sus veces, que deberán ser agrupados de la siguiente manera

2.8.1.1 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.

2.8.1.2 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,

2.8.1.3 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.

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: (1) diseño claro de los procesos, los cuales deben ser adaptables y dinámicos; (2) descripción en secuencia lógica y ordenada de las actividades, tareas, y controles; (3) 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; (4) difusión y comunicación de los procesos buscando garantizar su total aplicación; y, (5) 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 (gubernante, 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.

2.8.2 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:

2.8.2.1 Los procesos de incorporación.

Que comprenden la planificación de necesidades, el reclutamiento, la selección, la contratación e inducción de nuevo personal.

2.8.2.2 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,

2.8.2.3 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.

2.8.3 Tecnología de la Información

Las instituciones controladas deben contar con la tecnología de información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones.

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

Dichas políticas, procesos y procedimientos se referirán a:

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

- El apoyo y compromiso formal del directorio u organismo que haga sus veces y la alta gerencia.
- Un plan funcional de tecnología de información alineado con el plan estratégico institucional; y, un plan operativo que establezca las actividades a ejecutar en el corto plazo (un año), de manera que se asegure el logro de los objetivos institucionales propuestos.
- Tecnología de información acorde a las operaciones del negocio y al volumen de transacciones, monitoreada y proyectada según las necesidades y crecimiento de la institución.
- Un responsable de la información que se encargue principalmente de definir y autorizar de manera formal los accesos y cambios funcionales a las aplicaciones y monitorear el cumplimiento de los controles establecidos.
- Políticas, procesos y procedimientos de tecnología de información definidos bajo estándares de general aceptación que garanticen la ejecución de los criterios de control interno de eficacia, eficiencia y cumplimiento, debidamente aprobados por el directorio u organismo que haga sus veces, alineados a los objetivos y actividades de la institución.

- Difusión y comunicación a todo el personal involucrado de las mencionadas políticas, procesos y procedimientos, de tal forma que se asegure su implementación; y,
- Capacitación y entrenamiento técnico al personal del área de tecnología de información y de los usuarios de la misma.

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

- Manuales o reglamentos internos, debidamente aprobados por el directorio u organismo que haga sus veces, que establezcan como mínimo las responsabilidades y procedimientos para la operación, el uso de las instalaciones de procesamiento de información y respuestas a incidentes de tecnología de información.
- Un procedimiento de clasificación y control de activos de tecnología de información, que considere por lo menos, su registro e identificación, así como los responsables de su uso y mantenimiento, especialmente de los más importantes.

Con el objeto de garantizar que los recursos y servicios provistos por terceros, se administren con base en responsabilidades claramente definidas y estén sometidas a un monitoreo de su eficiencia y efectividad, las instituciones controladas deben contar al menos con lo siguiente:

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

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

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

- Políticas y procedimientos de seguridad de la información que establezcan sus objetivos, importancia, normas, principios, requisitos de cumplimiento, responsabilidades y comunicación de los incidentes relativos a la seguridad; considerando los aspectos legales, así como las consecuencias de violación de estas políticas.
- La identificación de los requerimientos de seguridad relacionados con la tecnología de información, considerando principalmente: la evaluación de los riesgos que enfrenta la institución; los requisitos legales, normativos, reglamentarios y contractuales; y, el conjunto específico de principios, objetivos y condiciones para el procesamiento de la información que respalda sus operaciones.
- Los controles necesarios para asegurar la integridad, disponibilidad y confidencialidad de la información administrada.
- Un sistema de administración de las seguridades de acceso a la información, que defina las facultades y atributos de los usuarios, desde el registro, eliminación y modificación, pistas de auditoría;

además de los controles necesarios que permitan verificar su cumplimiento en todos los ambientes de procesamiento.

- Niveles de autorización de accesos y ejecución de las funciones de procesamiento de las aplicaciones, formalmente establecidos, que garanticen una adecuada segregación de funciones y reduzcan el riesgo de error o fraude.
- Adecuados sistemas de control y autenticación para evitar accesos no autorizados, inclusive de terceros; y, ataques externos especialmente a la información crítica y a las instalaciones de procesamiento.
- Controles adecuados para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia, así como instalar y actualizar periódicamente aplicaciones de detección y desinfección de virus informáticos y demás software maliciosos.
- Controles formales para proteger la información contenida en documentos; medios de almacenamiento u otros dispositivos externos; el uso e intercambio electrónico de datos contra daño, robo, accesos, utilización o divulgación no autorizada de información para fines contrarios a los intereses de la entidad, por parte de todo su personal y de sus proveedores.
- Instalaciones de procesamiento de información crítica en áreas protegidas con los suficientes controles que eviten el acceso de personal no autorizado y daños a los equipos de computación y a la información en ellos procesada, almacenada o distribuida.

- Las condiciones físicas y ambientales necesarias para garantizar el correcto funcionamiento del entorno de la infraestructura de tecnología de información.
- Un plan para evaluar el desempeño del sistema de administración de la seguridad de la información, que permita tomar acciones orientadas a mejorarlo; y,
- Las instituciones controladas que ofrezcan los servicios de transferencias y transacciones electrónicas deberán contar con políticas y procedimientos de seguridad de la información que garanticen que las operaciones sólo pueden ser realizadas por personas debidamente autorizadas; que el canal de comunicaciones utilizado sea seguro, mediante técnicas de encriptación de información; que existan mecanismos alternos que garanticen la continuidad del servicio ofrecido; y, que aseguren la existencia de pistas de auditoría.

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

- Controles para minimizar riesgos potenciales de sus equipos de computación ante eventos imprevistos, tales como: fallas, daños o insuficiencia de los recursos de tecnología de información; robo; incendio; humo; inundaciones; polvo; interrupciones en el fluido eléctrico, desastres naturales; entre otros.
- Políticas y procedimientos de respaldo de información periódicos, que aseguren al menos que la información crítica pueda ser recuperada en caso de falla de la tecnología de información o con posterioridad a un evento inesperado.

- Mantener los sistemas de comunicación y redundancia de los mismos que permitan garantizar la continuidad de sus servicios; y,
- Información de respaldo y procedimientos de restauración en una ubicación remota, a una distancia adecuada que garantice su disponibilidad ante eventos de desastre en el centro principal de procesamiento.

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:

- 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.
- Documentación técnica y de usuario permanentemente actualizada de las aplicaciones de la institución.
- Controles que permitan asegurar la adecuada administración de versiones de las aplicaciones puestas en producción; y,
- Controles que permitan asegurar que la calidad de la información sometida a migración, cumple con las características de integridad, disponibilidad y confidencialidad.

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

2.8.4 Factores 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.

2.9 Identificación de riesgos.

Aplicando las definiciones anteriores los eventos de riesgos se subdividen en dos grandes grupos:

2.9.1 Riesgos Internos.

Son todos los riesgos cuya causa se da o identifica internamente en la Mutualista Imbabura y su impacto afecta directamente a sus resultados de la institución, entiéndase estos como las fallas en procesos personas y tecnología de la información.

2.9.2 Riesgos externos.

Son todos los eventos de riesgos que se suscitan de forma externa y que a su vez afectan la rentabilidad de la institución; entiéndase como tales a todos los desastres naturales, factores socioeconómicos y políticos y los ocasionados por proveedores externos indispensables o considerados críticos.

2.10 LÍNEAS DE NEGOCIO.

El documento Nuevo acuerdo de capitales Basilea II ha identificado 8 líneas de negocio como a continuación se enlistan.

- Finanzas Corporativas,
- Negociación y ventas,
- Banca minorista,
- Banca comercial,
- Pagos y liquidación,
- Servicios de agencia,
- Administración de activos,
- Intermediación minorista.

Cuadro No. 5. Proceso específicos para la administración de R O.

NIVEL 1	NIVEL 2	GRUPOS DE ACTIVIDADES
Finanzas Corporativas	<ul style="list-style-type: none"> • Finanzas Corporativas • Finanzas de administraciones locales / públicas • Banca de Inversión • Servicios de Asesoramiento 	Fusiones y adquisiciones, Suscripción de emisiones, privatizaciones, titularización, Servicio de estudios, deuda (pública alto rendimiento), acciones, sindicaciones, ofertas públicas iniciales, colocaciones privadas en mercados secundarios.
Negocios y Ventas	<ul style="list-style-type: none"> • Ventas • Creación de Mercado • Posiciones Propias • Tesorería 	Renta fija, renta variable, divisas, productos básicos, crédito, financiación, posiciones propias en valores, préstamo y operaciones con pacto de recompra, intermediación, deuda, intermediación unificada (prime brokerage)
Banca Minorista	<ul style="list-style-type: none"> • Banca Minorista • Banca Privada • Servicios de Tarjetas 	<ul style="list-style-type: none"> • Préstamos y depósitos de clientes minoristas, servicios bancarios, fideicomisos y testamentarias. • Préstamos y depósitos de particulares, Servicios Bancarios, fideicomisos y testamentarias, y asesoramiento de inversión. • Tarjetas de empresas / comerciales, de marca privada y minoristas.
Banca Comercial	<ul style="list-style-type: none"> • Banca Comercial 	Financiación de proyectos. Bienes raíces, financiación de exportaciones, factoring, arrendamiento financiero, préstamo, garantías, letras de cambio.
Liquidación y Pagos	<ul style="list-style-type: none"> • Clientes Externos 	Pagos y recaudaciones, transferencia de fondos, compensación y liquidación.
Servicios de Agencia	<ul style="list-style-type: none"> • Custodia • Agencia para empresas • Fideicomisos de empresas 	<ul style="list-style-type: none"> • Contratos, certificados de depósito, oper. de sociedades para préstamo de valores • Agentes de emisiones y pagos
Administración de Activos	<ul style="list-style-type: none"> • Administración discrecional de fondos • Administración no discrecional de fondos 	<ul style="list-style-type: none"> • Agrupados, segregados, minoristas, instituc., cerrados. Abiertos, part. Accionarias. • Agrupados, segregados, minoristas, instit., cap. Fijo, cap. Variable
Intermed. Minorista	Intermediación minorista	Ejecución y servicio completo

Fuente: Nuevo acuerdo de capitales

Elaboración: Basilea II

Para el desarrollo de la presente fue necesario identificar las líneas de negocio mediante las cuales opera Mutualista Imbabura divididas principalmente por su actividad económica y en consenso se define a como línea a Banca Minorista como la única línea de negocios en la que encaja la institución.

2.11 MEDICIÓN DE RIESGO OPERATIVO

Según lo publicado por el Club de Gestión de Riesgos de España (http://www.clubgestionriesgos.org/es/secciones/riesgo_operacional/introduccion/) Se proponen tres métodos para calcular los requerimientos de capital por riesgo operacional. En orden creciente de sofisticación y sensibilidad al riesgo, estos métodos son:

- El método del indicador básico;
- El método estándar;
- Los métodos de medición avanzada (AMA).

2.11.1 Método del indicador básico BIA.

El HSBS de México publica en su sitio web la siguiente información: (<http://www.riesgooperacional.com/docs/22%20%20gacetabasilea-II-no6-riesgo-operacional.pdf>)

El cálculo se realiza multiplicando un factor $\alpha = 15\%$ por promedio de los tres últimos años de los ingresos netos anuales positivos de la Institución. El cálculo tendrá un piso de 5% y un techo de 15% del promedio de los últimos 36 meses de los requerimientos de capital por riesgo de crédito y de mercado.

2.11.2 Método estándar.

En http://es.wikipedia.org/wiki/Riesgo_operativo se publica la definición del método estándar:

Bajo la metodología estándar, las actividades de los bancos se dividen en líneas de negocio. Se calculan los ingresos brutos de cada línea de negocio y a cada uno de estos se los multiplica por un factor (beta) que estima la exposición que tiene cada línea de negocio y permite calcular la provisión de capital para cada línea de negocio (finanzas corporativas: 18%; negociación y ventas: 18%; banca minorista: 12%, banca comercial: 12%; pagos y liquidación: 18%; servicios de agencia: 15%; administración de activos: 12%; intermediación minorista: 12%). Al final el requerimiento total de capital es la suma de los requerimientos de cada línea.

La última modificación a este concepto fue realizada el 9 de marzo del 2.013

2.11.3 Método de medición avanzada AMA.

Según Otero P. y Benerio O en su documento Metodología “Value at Risk” se refieren al método de medición avanzado AMA de riesgo operativo de la siguiente manera.

Calcula el capital de acuerdo a lo generado por el sistema interno de medición de cada institución. Si bien tiene la ventaja de ser más completo, en el sentido que abarca a la propia institución, tiene la gran desventaja que no existen muchos datos internos de pérdidas. Pág. 69

El cumplimiento de los requerimientos del organismo de control para adoptar cualquier de los métodos establecidos (Básico, Estándar y/o AMA) implica la implantación de una serie de requerimientos cuantitativos en la medición del nivel de riesgo y una serie de requerimientos cualitativos que incorporamos a continuación:

Cuadro No. 6. Requerimientos métodos de medición.

Criterios de admisión s/ Basilea II	Indicador Básico	Modelo Estándar	Modelo Avanzado	Comentarios
Cumplimiento de las "Sound Practices for the Management and Supervision of Operational Risk".	-	-	-	
Documentación de políticas, controles y procedimientos internos relativos al sistema de gestión del riesgo operacional.		-	-	MARCO DE GESTIÓN DEL RIESGO OPERACIONAL
Asignación de responsabilidades claras a la Unidad de Gestión del Riesgo Operacional.		-	-	
Validación y exámen periódico independiente de los procesos de gestión y sistemas de evaluación del riesgo operacional.		-	-	
Recursos suficientes para aplicar la metodología en las principales líneas de negocio y en los ámbitos de control y auditoría		-	-	ASIGNACIÓN DE RECURSOS
Participación activa del Consejo de Administración y de la Alta Dirección en la vigilancia del marco de gestión.		-	-	
Sistema de gestión conceptualmente sólido y aplicado en su totalidad.		-	-	CUADRO DE MANDO DE RIESGO OPERACIONAL
Sistema periódico de reporting a la dirección de las unidades de negocio, a la Alta Dirección y al Consejo de Administración.		-	-	
Análisis sistemático de las pérdidas relevantes en cada		-	-	BASE DE DATOS DE PÉRDIDAS

línea de negocio.		
Sistema de gestión del riesgo operacional perfectamente integrado dentro de los procesos de gestión del riesgo de la Entidad.	-	- SISTEMAS DE MEJORA CONTINUA
Utilización, en el sistema de cálculo del riesgo operacional, de análisis de escenarios y factores que reflejen el entorno del negocio y los sistemas de control interno.		- METODOLOGÍAS CUALITATIVAS (CUESTIONARIOS, KRI's)
Utilización, en el sistema de cálculo del riesgo operacional, de datos internos y datos externos.		-
Identificación de eventos situados en las "colas" de la distribución de probabilidad (criterio de solidez).		-
Cálculo basado en 5 años mínimo de observación de datos internos de pérdida (3 años la primera vez que se utilice el modelo avanzado).		- METODOLOGÍAS CUANTITATIVAS, MOTOR DE CÁLCULO
Integridad de los datos internos de pérdida. Establecimiento de un umbral mínimo para la recopilación de datos.		-
Metodologías de incorporación de datos externos y procedimientos periódicos de revisión de la adecuación de los mismos.		- METODOLOGÍAS CUANTITATIVAS, DATOS EXTERNOS

Fuente: Club de Gestión de Riesgos de España

Elaboración: Club de Gestión de Riesgos de España

2.12 TEMAS RELACIONADOS A RIESGO OPERATIVO

2.12.1 Planes de continuidad del negocio.

Según resolución JB-834 de riesgo operativo de la Superintendencia de Bancos y Seguros del Ecuador se considera entre otras cosas que:

Continuidad del Negocio es un concepto que abarca tanto la Planeación para Recuperación de Desastres (DRP) como la Planeación para el Restablecimiento del Negocio. Recuperación de Desastres es la capacidad para responder a una interrupción de los servicios mediante la implementación de un plan para restablecer las funciones críticas de la organización. Ambos se diferencian de la Planeación de Prevención de Pérdidas, la cual implica la calendarización de actividades como respaldo de sistemas, autenticación y autorización (seguridad), revisión de virus y monitoreo de la utilización de sistemas.

Plan de Continuidad del Negocio (BCP) son los planes logísticos para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre. Estos planes son llamados Planes de Continuidad del Negocio, según publicación de: http://es.wikipedia.org/wiki/Plan_de_continuidad_del_negocio

El documento del plan de continuidad de negocio debe contar con mecanismos, estrategias y políticas que aseguren la NO interrupción de la las operaciones diarias de la Mutualista Imbabura. Toda institución financiera de acuerdo a la resolución No. JB-2005-834 de 20 de Octubre del 2005 deben implementar planes de continuidad de negocio para la prevención y litigación de los impactos generados por eventos de riesgo operativo.

2.12.2 Planes de seguridad de la Información

Según lo señalado en la norma ISO/IEC 27001, Seguridad de la Información seguridad de la información se define como:

En la actualidad las empresas se enfrentan cada vez más con riesgos e inseguridades procedentes de una amplia variedad de fuentes que pueden dañar de forma importante sus sistemas de información y pueden poner en peligro la continuidad del negocio

Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la autenticidad e Integridad de la misma.

Grafico No. 7. Seguridad de la información.



Fuente: <http://moodlexa.unsa.edu.ar/course/info.php?id=53>

Elaboración: Comisión de seguridad de la información.

Para el caso de Mutualista Imbabura se cuenta con personal asignado específicamente para esta actividad la cual se encuentra normada dentro de un manual como parte del cumplimiento del plan integral de Riesgo Operativo

2.12.3 Planes de contingencia.

Según lo que se publica en el sitio web de Bridged World se define un plan de contingencia como:

La definición de Contingencia está vinculada al riesgo, y es la posibilidad de que algo pueda suceder. Un Plan de Contingencias es el instrumento donde se diseña la estrategia, se recogen todas las medidas organizativas y técnicas, y se exponen los procedimientos para enfrentarse a la eventualidad de un riesgo o un imprevisto que ponga en peligro la continuidad de la actividad en una organización.

<http://www.bridgedworld.com/es/soluciones/planes-de-contingencia>

La función principal de un Plan de Contingencia es la continuidad de las operaciones de la institución su elaboración la dividimos en cuatro etapas:

- Evolución,
- Planificación,
- Viabilidad,
- Ejecución.

Las tres primeras hacen referencia al componente preventivo y la última a la ejecución del plan una vez ocurrido el siniestro o el evento. La planificación aumenta la capacidad de organización en caso de siniestro sirviendo como punto de partida para las respuestas en caso de emergencia.

Se identificaran los posibles riesgos y se delimitaran las tareas para solucionar o corregir el impacto

Cuadro No. 8. Ejemplo de levantamiento de riesgos.

RIESGOS	LOCALIZACIÓN
Incendios	Sitios de almacenamiento y manipulación de Combustibles.
Falla de estructuras	Estribos, cimentación, estructuras de las bases de las torres.
Derrame de combustibles	Sitios de almacenamiento y manipulación de combustibles.
Accidentes de trabajo	Se pueden presentar en todos los frentes de obra.
Enfermedades y epidemias	Campamentos y pueblos cercanos.
Fallas en el suministro de insumos	Todo el Proyecto podría verse afectado.
Huelga de trabajadores	Cualquier parte del Proyecto podría verse afectado.
Paro cívico	Cualquier parte del Proyecto podría verse afectado.

Fuente: http://www.abc.gob.bo/IMG/pdf/Cap_8-_SBX_Plan_de_contingencias.pdf

Elaboración: EEIA PLAN DE CONTINGENCIAS

2.13 TEMAS RELACIONADOS AL PROYECTO DE TESIS

2.13.1 Diagnóstico.

Según publicación del sitio <http://definicion.de/diagnostico/> el diagnóstico será definido como:

Diagnóstico es una palabra que tiene su origen etimológico en el griego y más aún en la unión de tres vocablos de dicha lengua. En concreto, es un término que está formado por el prefijo diag- que significa “a través de”; la palabra gnosis que es un sinónimo de “conocimiento”, y finalmente el sufijo -tico que se define como “relativo a”.

Un diagnóstico es aquello que, en el ámbito de la medicina, está vinculado a la diagnosis. Este término, a su vez, hace referencia a diagnosticar: recabar datos para analizarlos e interpretarlos, lo que permite evaluar una cierta condición.

Del diagnóstico realizado se pueden identificar las fortalezas, oportunidades debilidades y amenazas principales que se han obtenido luego de la utilización de los instrumentos de recolección de datos mismas que sirven de insumo para el desarrollo de la propuesta.

2.13.2 Análisis de impactos.

Según se define mediante lo publicado en la siguiente dirección: http://www.corporacionsybven.com/portal/index.php?option=com_content&view=article&id=238: analisis-de-impacto&catid=124:conceptos-teoricos. El análisis de impacto consiste en conocer la relación entre los resultados existentes y las consecuencias para determinar condiciones positivas o negativas que afecten al proyecto.

En la presente tesis se consideran como impactos los factores de riesgo operativo los cuales son las fallas en procesos, personas, tecnología de información y eventos externos, teniendo una limitante en este último factor puesto que se trata de un tema subjetivo que impide una visualización integral de cada uno de los eventos que podrían suscitarse; dejando a un lado los impactos tradicionales, por ende en el capítulo correspondiente se consideran los impactos en procesos, personas y tecnología de información.

CAPÍTULO III

3 PROPUESTA.

Con el desarrollo del presente trabajo de investigación se propone la elaboración del siguiente **“MANUAL DE RIESGO OPERATIVO PARA LA MUTUALISTA IMBABURA”**

3.1 INTRODUCCIÓN.

El Riesgo Operativo se lo encuentra inherente todo negocio o actividad, el cual actualmente se manifiesta en mayor grado o frecuencia, principalmente por la incidencia de diversos factores como las mejoras tecnológicas y la creciente globalización del sistema financiero y comercial. La mayor dependencia que las organizaciones tienen es de los procesos informáticos, el desarrollo del comercio electrónico, el crecimiento del volumen de operaciones, la transaccionalidad y la complejidad cada vez mayor de las operaciones.

Por tal razón la aparición de nuevas técnicas de identificación, control y mitigación cobra relevancia e impone una rápida puesta en marcha de las mismas a fin de disminuir la probabilidad de ocurrencia y el nivel de impacto de los eventos de riesgo detectados, evitando así que la institución incurra en pérdidas económicas o que estas sean aceptables y no represente mayor perjuicio para la institución.

Mutualista Imbabura delimita su accionar para la administración de riesgo operativo de acuerdo a lo que se desglosa a continuación:

3.2 GENERALIDADES.

3.2.1 Objetivo general.

Establecer las políticas y procedimientos para una adecuada Gestión de Riesgos Operativos mediante la creación de la infraestructura y la cultura organizacional adecuada que permitan la aplicación de un método adecuado para principalmente: identificar, analizar, evaluar, mitigar, monitorear, controlar y comunicar los riesgos operativos asociados con fallas o insuficiencias causadas por procesos, personas, tecnología de información (hardware y software) y eventos externos que principalmente ocasionen una posible pérdida económica para la Mutualista Imbabura.

3.2.2 Objetivos específicos.

- Identificar las políticas específicas para administrar los riesgos originados que afectan negativamente la eficiencia en el desarrollo de las actividades institucionales.
- Delimitar las funciones y responsabilidades de cada uno de los autores dentro de la organización.
- Definir el proceso general para la administración de riesgo operativo dentro de la Mutualista Imbabura.
- Determinar la gestión metodológica y los procedimientos específicos para la administración de riesgo operativo dentro de la institución.

3.3.3 Alcance.

Las disposiciones del presente manual son aplicables dentro de la estructura orgánico-funcional de la Mutualista Imbabura, sus áreas

comerciales y operativas, productos, servicios, personas, sistemas, eventos externos y procesos estableciendo las pautas necesarias para los aspectos técnicos y metodológicos de acuerdo a su estructura organizacional.

El manual ha sido desarrollado tomando como base las resoluciones de la Junta Bancaria N° JB-2005-834 y N° JB-2008-1202 emitidas por la Superintendencia de Bancos y Seguros del Ecuador, y el informe de Convergencia Internacional de Medidas y Normas de Capital elaborado por el Comité de Supervisión Bancaria de Basilea.

3.4 POLÍTICAS PARA LA ADMINISTRACIÓN DE RIESGO OPERATIVO.

3.4.1 Política General.

El Directorio de Mutualista Imbabura impulsará a todos los núcleos organizacionales la cultura de la gestión de los riesgos operativos buscando así minimizar las pérdidas por la exposición a los eventos de este riesgo.

3.4.2 Políticas específicas.

- Los órganos de administración y de control de la institución deberán asegurar el cumplimiento de las normas internas y externas relacionadas con la administración del riesgo operativo.
- Implementar procedimientos para la identificación de riesgos operativos y la recolección de información especialmente para el registro de eventos de riesgo
- Promover la implementación de controles a fin de mitigar la exposición de la organización al riesgo operativo.

Cuadro No. 9. Formato de evaluación Políticas específicas

FORMATO DE EVALUACIÓN DE CUMPLIMIENTO DE POLÍTICAS ESPECÍFICAS DE RIESGO OPERATIVO						
ÁREA RESPONSABLE DEL CUMPLIMIENTO: _____						
FECHA DE REALIZACIÓN: _____						
#	ACTIVIDAD	INCUMPLIDA	CUMPLIMIENTO PARCIAL	CUMPLIMIENTO TOTAL	ACTIVIDADES PENDIENTES	PERSONAL RESPONSABLE DEL CUMPLIMIENTO
1	El directorio monitorea de manera periódica el cumplimiento de las normas internas y externas relacionadas con la administración de riesgo operativo					PRESIDENTE DEL DIRECTORIO
2	Se han implementado por parte del Directorio procedimientos para la implementación de riesgos operativos					DELEGADO DEL DIRECTORIO
3	Analizar los controles de manera periódica para mitigar la exposición al riesgo operativo					PRESIDENTE DEL COMITÉ DE RIESGOS
ELABORADO POR:		REVISADO POR:			APROBADO POR:	

Fuente: Autor del proyecto

Elaboración: Autor del Proyecto

3.4.3 Políticas aplicables a la generación del árbol de procesos.

- Se deberá definir una estrategia de identificación de los nuevos procesos de Mutualista Imbabura basados en las necesidades institucionales, para establecer las áreas del negocio que participan en el proceso.
- Establecer la naturaleza del proceso de acuerdo al rol que desempeñan dentro de la institución y clasificarlos en procesos productivos, de apoyo a la gestión o gobernantes.
- Analizar la importancia de los procesos, estableciendo sus niveles de criticidad.
- Identificar los procesos críticos de la entidad asociados a la línea de negocio que pertenecen
- Identificar los procesos provistos por terceros y asociarlos a una matriz de riesgos por proveedor.

3.4.4 Políticas aplicables a la identificación de riesgos.

- La Unidad de riesgos realizará un levantamiento de los riesgos inherentes a cada uno de los procesos conjuntamente con los dueños de los mismos; este levantamiento deberá ser actualizado al momento que se actualicen los procesos.
- Para cada riesgo identificado se deberá definir un valor de severidad y un número de frecuencias.

- La probabilidad o frecuencia de ocurrencia de los riesgos, deberá expresarse en un número anual de ocurrencias.
- La severidad de los riesgos identificados debe estar expresada en valores monetarios de acuerdo a la moneda de uso oficial.
- La solidez de un control o conjunto de controles, deberá reflejar las expectativas del usuario respecto a dicho control y luego será calibrada con el resultado real de su aplicación, y así controlar la evolución de la exposición al riesgo.
- Los controles tienen como objetivo reducir la probabilidad de ocurrencia de los eventos mientras que las mitigaciones se encargan de reducir la severidad en términos monetarios.
- Se considerarán para efectos del riesgo operativo como mitigaciones a los seguros, documentos o bienes de respaldo bajo la modalidad de garantía ante la ocurrencia o materialización de un evento de riesgo.
- Diseñar por parte de la Unidad de Riesgos mecanismos de reportes de eventos de riesgo por parte del personal que llegare a cometer errores o a su vez por sus supervisores o jefes inmediatos, generando así un adecuado ambiente de control en todos los niveles de la institución

3.4.5 Políticas aplicables a la selección del método de evaluación de riesgos.

- Se identificará por parte del responsable de la Unidad de Riesgos las características relevantes de los eventos de riesgo para su documentación y registro (Número de ocurrencias anuales,

severidad en términos monetarios, identificación del evento de riesgo, entre otros).

- Establecer mecanismos de relevamiento de información de los riesgos identificados en la institución, tanto de forma cualitativa como cuantitativa.
- Los riesgos cuya severidad sea mínima (a criterio del responsable de la unidad de riesgos), únicamente serán legalizados mas no gestionados mediante la ejecución de planes de acción.
- Trabajar con análisis cualitativo como proceso inicial para conocer la realidad institucional y su nivel de exposición original, y definir en función de este análisis, la estructura que deben tener los riesgos para documentarlos y preparar a la institución para un proceso de análisis cuantitativo a futuro.

3.4.6 Políticas aplicables a la identificación de controles y mitigaciones.

- Se deberá mantener por parte de la Unidad de Riesgos un inventario de controles con los que cuenta actualmente la institución. Posteriormente la institución deberá analizar los controles que sean factibles de implementar en el corto y mediano plazo. Se recomienda iniciar el análisis con los controles de corto plazo con el fin de evitar la materialización de eventos de mayor impacto.
- Identificar el grado de eficiencia, diseño y solidez de cada uno de los controles, basándose en los resultados de disminución o incremento de frecuencia y severidad de los eventos a juicio y criterio del evaluador.

- Construir indicadores de desempeño para medir la eficiencia de los controles y planificar metas del indicador para su seguimiento.

3.4.7 Políticas aplicables al análisis de riesgos.

- Realizar periódicamente el levantamiento de información respecto a los riesgos identificados dentro de cada una de las actividades de los procesos con los que cuenta la institución, para realizar valoraciones cualitativas de los riesgos en términos de probabilidad de ocurrencia y severidad monetaria.
- Analizar la evolución histórica de las concentraciones de riesgo, para determinar la cantidad de riesgos a atender en el tiempo. Se procederá a analizar los valores del riesgo bruto, y obtener como indicador de desempeño una relación entre cada estado sobre el total de sus riesgos.
- Las metas de los indicadores de desempeño, deben enfocarse principalmente en los riesgos críticos y su meta será reducirlos en el tiempo tanto en severidad como en frecuencia precautelando así los resultados de la institución.
- En caso de no existir riesgos operativos que sean considerados como críticos se realiza el análisis detallado a los de mayor frecuencia.
- Los eventos detectados en el área de ventanillas en los cuales su reposición fue efectuada por el personal responsable del evento se lo deberá recuperar a pesar de que se haya recuperado el valor.
- De existir otros eventos que generan pérdidas asociados a otros procesos diferentes a los de ventanilla cuya pérdida monetaria sea

cubierta por el personal responsable se deberán considerar de igual manera como en el enunciado anterior.

- Realizar el análisis de los mapas de riesgos brutos y residuales con diversos modelos internos para establecer el impacto de los riesgos bajo diferentes escenarios. Para esto es importante elaborar modelos donde varíen las probabilidades de ocurrencia y severidades.

3.4.8 Políticas aplicables a la evaluación del riesgo operativo.

La exposición al riesgo operativo deberá ser planteada teniendo en cuenta que:

- Los riesgos deben ser tomados con moderación de acuerdo al apetito de riesgos de la institución.
- Los riesgos tomados deben medirse bajo una base común (impacto monetario).
- Los riesgos deben recibir una supervisión adecuada por parte de las áreas responsables de acuerdo al tipo de riesgo.
- Se informara oportunamente a las diferentes áreas involucradas sobre los cambios en materia de frecuencia y severidad de los mismos.
- Los riesgos deberán cumplir estrictamente con las limitaciones contenidas en la normativa y la legislación vigentes.

Los principios de la política de riesgos de las actividades de Mutualista Imbabura se basan en:

- Excelencia e integridad en las operaciones.
- Equilibrar la toma de riesgos con controles apropiados.
- Importancia de la disciplina y respeto hacia los límites establecidos para cada uno de los riesgos.
- Diversificar las actividades para evitar una innecesaria concentración de riesgos.
- Equilibrar la dependencia en los modelos estadísticos de cuantificación de pérdida esperada con el uso del buen juicio del responsable de la administración de riesgo operativo.
- Mantener una comunicación eficaz y adecuada dentro de todas las áreas de la institución.
- Una vez establecidos los mapas de riesgos, el Comité de Riesgos deberá proponer los límites de exposición al riesgo operativo considerados como aceptables.
- Será misión de la Unidad de Riesgos fijar la prioridad de tratamiento y los mecanismos de mitigación para aquellos riesgos que se encuentren excedidos de los valores fijados.

3.4.9 Políticas aplicables al tratamiento de los riesgos.

- Establecer la relación entre los mapas de riesgos brutos y residuales con el tratamiento del riesgo, a efectos de decidir las acciones a tomar con las concentraciones de riesgos determinadas (reducir, aceptar, transferir, evitar).

- Analizar alternativas de tratamiento proactivo ante riesgos futuros, basadas en la concentración de riesgos existente y en el conocimiento de los mercados.
- Se establecerá por parte de la Unidad de Riesgos prioridades de acción frente al tratamiento del riesgo, orientando los esfuerzos a los riesgos más críticos.

3.4.10 Políticas aplicables al monitoreo de los riesgos.

- Establecer indicadores de desempeño, basados en la probabilidad de ocurrencia de los riesgos, poniendo énfasis en los riesgos más críticos. La estrategia de estos indicadores, es utilizar controles y la meta es disminuir la ocurrencia y la severidad.
- Establecer indicadores de desempeño, poniendo énfasis en los riesgos más críticos.
- El cumplimiento de las metas y resultados debe medirse al menos en cada trimestre del año, adecuando los controles y mitigaciones de los riesgos en el caso de que en dos trimestres seguidos la meta no haya evolucionado.
- La Unidad de Riesgos de manera anual deberá cuantificar el costo anual del control que se debe a implementar.
- Considerar en el monitoreo, el costo del control vs. la severidad monetaria. El costo anual del control deberá representar una porción del costo de ocurrencia anual del evento de riesgo que controla. Si esto no ocurre, se deben calibrar los modelos de riesgos brutos y residuales y revisar la eficiencia de los controles implementados.

- Revisar periódicamente en caso de que existan cambios en los mecanismos de análisis y medición de riesgos, sean estos solicitados por los organismos de control, sugeridos por metodologías de aplicación internacional o por las recomendaciones de las diferentes auditorías.

3.4.11 Políticas aplicables a la comunicación y divulgación de resultados.

- Las políticas establecidas con respecto a la comunicación y divulgación de resultados están orientados a la aplicación de la metodología propia de la institución, las mismas deben traducirse en reglas de conducta y procedimientos que orienten la actuación de cada uno de los funcionarios de la organización y deberán cumplir los siguientes requisitos:
- Elaborar informes internos y externos para la divulgación de los resultados obtenidos.
- Mantener comunicadas a las áreas de negocio con la Unidad de Riesgos respecto de la evolución de los riesgos y su tratamiento.
- Definir acciones a tomar para reducir los riesgos brutos y residuales, de acuerdo a los indicadores de desempeño elaborados y conforme a las necesidades institucionales. Todo control y/o mitigación debe analizarse tanto en cumplimiento de resultados (metas) como en costo monetario, para establecer su solidez real.
- Apoyar a las áreas de negocio en la divulgación de la efectividad de los controles / mitigaciones, estableciendo un único canal formal para la divulgación de resultados oficiales.

- Cumplir adecuadamente con los requerimientos de información solicitados por los organismos de control en tiempo y forma.

3.4.12 Políticas aplicables a la gestión para la creación de nuevos productos y servicios.

- El responsable de la administración de riesgo operativo será quien realice la identificación de los riesgos inherentes a la implementación de nuevos productos y servicios, basados en su juicio y criterio.
- Determinar la misión del producto o servicio y los procesos con los que interactúa, estableciendo las áreas involucradas en su administración, su marco legal de implementación y su flujo operativo, para esto se deberá tomar en consideración el criterio de las áreas involucradas.
- Analizar los controles y acciones mitigadoras existentes, que puedan apoyar a la gestión de nuevos productos y servicios dentro de la institución.

3.4.13 Políticas aplicables a la capacitación.

- Capacitar de manera anual al personal de la unidad de riesgos sobre temas relacionados al riesgo operativo.
- Generar una cultura de manejo e identificación de los riesgos en la Mutualista Imbabura, permitiendo que el personal se involucre en la gestión de riesgos de manera activa y conozca los riesgos y los controles implementados.

- Capacitar periódicamente al personal y directorio de la entidad en la gestión proactiva que permita evitar riesgos o disminuirlos adecuadamente con una periodicidad de por lo menos un año.
- A modo de inducción se dará a conocer a todo el personal nuevo de la institución, los lineamientos del proceso de administración de riesgos operativos.
- Siempre se dejará constancia mediante un control de asistencia de las inducciones o capacitaciones realizadas al personal de la institución, el cual deberá ser custodiado por la unidad de riesgos.
- En caso de regulaciones normativas que modifiquen el control y administración de riesgo operativo es obligación de la administración de Mutualista Imbabura buscar opciones de capacitación de manera inmediata.

Cuadro No. 10. Formato de evaluación Políticas específicas

FORMATO DE EVALUACIÓN DE CUMPLIMIENTO DE POLÍTICAS APLICABLES POR ÁREA O ACTIVIDAD						
ÁREA RESPONSABLE DEL CUMPLIMIENTO: _____						
FECHA DE REALIZACIÓN: _____						
#	ACTIVIDAD A EVALUAR	INCUMPLIDA	CUMPLIMIENTO PARCIAL	CUMPLIMIENTO TOTAL	ACTIVIDADES PENDIENTES	PERSONAL RESPONSABLE DEL CUMPLIMIENTO
1	Se cuenta con un árbol de procesos debidamente aprobado					RESPONSABLE DE PROCESOS
2	La probabilidad de ocurrencia se encuentra expresada en numero anual de ocurrencias					OFICIAL DE RIESGOS
3	La severidad se encuentra expresada en valores monetarios.					OFICIAL DE RIESGOS
4	Cuenta con controles debidamente definidos para reducir la probabilidad de ocurrencia					AUDITOR INTERNO
5	Se mantiene una herramienta informática que permita la selección de métodos de evaluación de riesgo operativo					OFICIAL DE RIESGOS
6	Se encuentra levantado un inventario de controles en la institución					AUDITOR INTERNO
7	Son analizados los controles existentes para determinar su factibilidad al corto plazo					COMITÉ DE RIESGOS
8	Se ha definido el grado de eficiencia solidez y diseño de los controles.					COMITÉ DE RIESGOS
9	Existen indicadores de desempeño para medir la eficiencia de los controles					OFICIAL DE RIESGOS
10	Se levanta periódicamente la información respecto a los riesgos identificados dentro de los procesos					OFICIAL DE RIESGOS
11	La principal fuente de información son los informes del Auditor interno, Oficial de Cumplimiento y Atención al cliente.					OFICIAL DE RIESGOS
12	Se aplican los mecanismos de evolución de riesgos					OFICIAL DE RIESGOS
13	Se han identificado límites de exposición de riesgo operativo					COMITÉ DE RIESGOS
14	Se dan prioridad a los riesgos mas críticos identificados en la institución					COMITÉ DE RIESGOS
15	Cuenta con mapas de riesgos brutos y residuales para medir la evolución de los riesgos					OFICIAL DE RIESGOS
16	Se informa al Comité de riesgos sobre la evolución de los riesgos operativos detectados.					OFICIAL DE RIESGOS
17	Se da a conocer a los organismos internos y externos sobre los resultados obtenidos de la administración de riesgos					OFICIAL DE RIESGOS
18	Los nuevos productos son analizados por la Unidad de riesgos					OFICIAL DE RIESGOS
19	Los nuevos productos son analizados por el Asesor Jurídico					ASISTENTE JURÍDICO
20	El área de procesos ha definido los procesos operativos de lo nuevos productos					RESPONSABLE DE PROCESOS
21	El personal es capacitado periódicamente en temas relacionados a riesgo operativo					JEFE DE TALENTO HUMANO
ELABORADO POR:		REVISADO POR:			APROBADO POR:	

Fuente: Autor del proyecto

Elaboración: Autor del Proyecto.

3.5 FUNCIONES Y RESPONSABILIDADES DE LA ORGANIZACIÓN.

3.5.1 Del Directorio de Mutualista Imbabura.

En cumplimiento de lo dispuesto en las resoluciones de la Junta Bancaria JB-2005-834 sobre riesgos; el Directorio de la institución fija las siguientes funciones y responsabilidades para la medición y control del riesgo operativo.

El Directorio y la Gerencia General administrará el riesgo operativo de la Mutualista Imbabura en su totalidad, para ello se basará en los siguientes análisis conceptuales:

- El comité de riesgos planteará al Directorio de Mutualista Imbabura que evalúe las políticas, procesos y procedimientos de la Administración del Riesgo Operativo y que sean implementados en toda la institución para que el personal de todos los niveles se relacione con las responsabilidades que conlleva el Riesgo Operativo.
- Mutualista Imbabura debe establecer y mantener un sistema que permita identificar, registrar, medir, monitorear y controlar los Riesgos Operativos, asignar un área responsable de la administración y mantenimiento del sistema que verifique el cumplimiento de las normas internas y externas que se establezcan.
- El sistema para la administración de riesgo operativo debe ser dinámico de tal forma que se asegure la identificación de cambios en los controles y perfiles de riesgo y permitir la actualización del nivel de riesgo operativo de Mutualista Imbabura, permitiendo a su vez la prevención y resolución de conflictos de interés en la

recolección de la información durante sus diferentes etapas de implementación, así como en el registro de eventos y en el mantenimiento del sistema.

- La Administración de Riesgo Operativo debe archivar bases de datos con información suficiente y oportuna, que contengan información sobre contrapartes, clientes, intermediarios, carteras, etc., y que a futuro permita estimar las pérdidas esperadas e inesperadas atribuibles a este riesgo.
- Especificar los métodos para la evaluación y rastreo de cambios significativos y a su vez la exposición a riesgos.
- Someter a aprobación del directorio de Mutualista Imbabura la evaluación de los planes de Contingencia y de Continuidad de Negocio que se hicieren por el comité de Riesgos.
- El Comité de Riesgos será el encargado de designar a los líderes encargados de hacer que las actividades expuestas en el plan de contingencias y de continuidad de negocios se cumplan y llevar al análisis y posteriormente a la aprobación de esta designación por parte del directorio de Mutualista Imbabura.
- Es responsabilidad del Comité de Riesgos de Mutualista Imbabura controlar en forma mensual el grado de cumplimiento del plan de riesgo operativo.
- La Unidad Integral de Riesgos será responsable de administrar la información de riesgo operativo, y a su vez apoyará en la identificación de los eventos de riesgo, en el diseño de los planes de acción, en el registro de dichos eventos y en el seguimiento a los resultados de los indicadores y planes de acción.

- Auditoría Interna deberá realizar una evaluación periódica para mejorar la efectividad de la administración de riesgo operativo; aclarando que no es directamente responsable de la gestión de implementación del plan de riesgo operativo o de ningún otro riesgo.

3.5.2 Funciones.

- Aprobar las políticas, estrategias y procedimientos, que permitan un adecuado manejo de los riesgos operativos, las mismas que deberán ser actualizadas permanentemente de acuerdo a las situaciones que se prevea puedan presentarse. Estas políticas, estrategias y procedimientos deberán ser compatibles con el volumen y complejidad de las operaciones que realiza la institución.
- Informarse periódicamente y al menos mensualmente, acerca de la implementación y el cumplimiento de las políticas, estrategias y procedimientos por ellos aprobadas;
- Establecer las acciones correctivas en caso de que las políticas, estrategias y procedimientos no se cumplan o se cumplan parcialmente, o incorrectamente;
- Establecer límites de exposición generales dentro de un rango prudencial para la administración de los riesgos en la entidad, compatibles con las actividades, estrategias y objetivos institucionales y que permitan una eficaz reacción frente a situaciones adversas.
- Informarse regularmente con una frecuencia de al menos una vez al mes, sobre la evolución de los riesgos de mercado, así como

sobre los cambios sustanciales de tal situación y de su evolución en el tiempo;

- Crear una cultura organizacional con principios y valores de comportamiento ético que priorice la gestión eficaz de prevención de la exposición al riesgo operativo;
- Aprobar las disposiciones relativas a los procesos establecidos en el numeral 4.1 del artículo 4 de la gestión de riesgo operativo, (capítulo incluido en la resolución No JB-2005-834 del 20 de octubre del 2005);
- Aprobar las políticas, procesos y procedimientos para la administración del Recurso humano con el que cuenta la Mutualista Imbabura;
- Aprobar las políticas y procedimientos para la administración de la tecnología de la información;
- Aprobar los planes de contingencia de tecnología y de continuidad del negocio de acuerdo a lo establecido en artículos 15 y 16 (artículos reenumerados con resolución No. JB-2008-1202 de 23 de octubre del 2008).

3.5.3 Comité de Riesgos.

3.5.3.1 Integrantes

Se designa a los siguientes miembros que conformarán el Comité Integral de Riesgos dentro de la institución los cuales tendrán las funciones que a continuación les serán asignadas:

- Vocal del Directorio de la Institución quien lo presidirá el Comité de Riesgos,
- Gerencia General,
- Responsable de la Unidad de Riesgos, persona calificada cuyos estudios sean Finanzas y temas afines,
- Jefes de oficina,
- Auditor Interno y
- Contador General.

El Comité de Riesgos sesionará con la mitad más uno de sus integrantes, sus decisiones las tomará por mayoría simple de votos; y, el Presidente del Comité tendrá voto dirimente.

Actuará como coordinador del Comité, el Responsable de la Unidad de Riesgos (oficial de riesgos), quien actuará además como Secretario de dicho Comité y se encargará de la elaboración de las actas y los informes internos y externos que le sean requeridos. Esta nómina será puesta en conocimiento de la Superintendencia de Bancos y Seguros con la periodicidad que esta lo requiera, acompañando la respectiva acta de sesión de Directorio en donde se haya procedido a nombrar a los integrantes.

3.5.3.2 Funciones.

Tendrá las siguientes funciones mínimas según lo señalado por la Superintendencia de Bancos y Seguros:

- Diseñar las políticas y el proceso de administración de riesgo operativo;
- Monitorear y evaluar los cambios significativos y la exposición a riesgos provenientes de los procesos, las personas, la tecnología de información y los eventos externos;
- Analizar las políticas y procedimientos de tecnología de información, propuestas por el área respectiva, especialmente aquellas relacionadas con la seguridad de la información;
- Conjuntamente con los informes de la unidad de riesgos de deberá liderar el desarrollo, la aplicabilidad y el cumplimiento de los planes de contingencia y continuidad del negocio; así como proponer los líderes de las áreas que deben cubrir el plan de contingencias y de continuidad de negocio.
- Elaborar las actualizaciones en el manual respecto del riesgo operativo, los que deben recoger las políticas, estrategias y procedimientos elaborados por el directorio o el organismo que haga sus veces, los mismos que deberán ser puestos en conocimiento de la Superintendencia de Bancos y Seguros así como las reformas que en ellos se produzcan.

3.5.4 Unidad de Riesgos.

3.5.4.1 Funciones.

- Diseñar las políticas y el proceso de administración del riesgo operativo;
- Elaborar y someter a consideración y aprobación del Comité de Riesgos la metodología para identificar, medir, controlar / mitigar y

monitorear los diversos riesgos asumidos por la Mutualista Imbabura en sus operaciones.

- Monitorear y evaluar los cambios significativos y la exposición a riesgos provenientes de los procesos, las personas, la tecnología de información y los eventos externos;
- Calcular las posiciones de riesgo y su afectación al patrimonio técnico de la entidad.
- Analizar las políticas y procedimientos de tecnología de información, propuestas por el área respectiva, especialmente aquellas relacionadas con la seguridad de la información; y,
- Liderar el desarrollo, la aplicabilidad y cumplimiento de los planes de contingencia y de continuidad del negocio; así como proponer los líderes de las áreas que deban cubrir el plan de contingencias y de continuidad del negocio.
- Realizar informes periódicos sobre el seguimiento a la exposición al riesgo operativo.

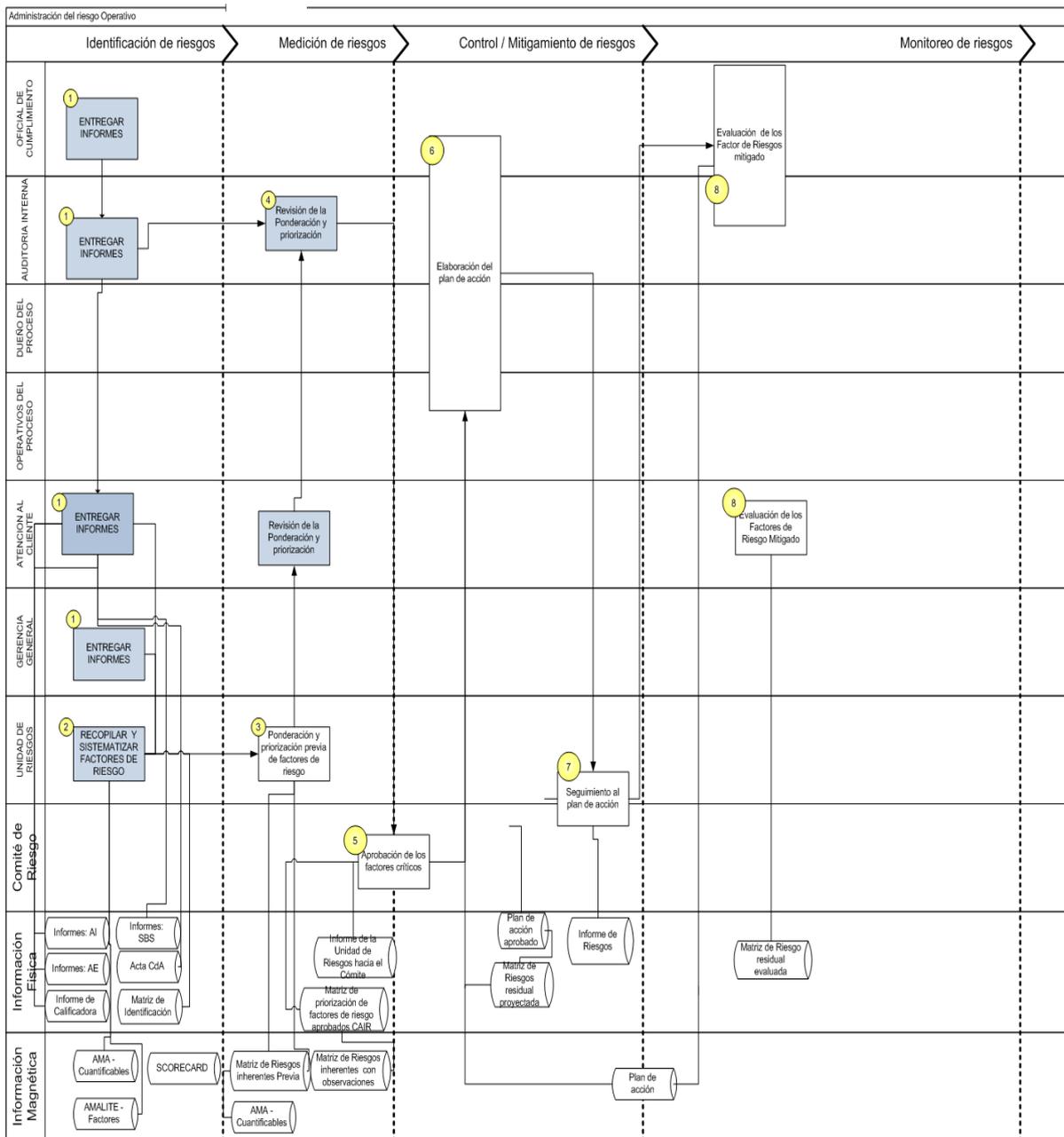
3.6 PROCESO GENERAL PARA LA ADMINISTRACIÓN DE RIESGO OPERATIVO.

A continuación la descripción gráfica del Proceso General de Administración del Riesgo Operativo de Mutualista Imbabura:

Este proceso será puesto a conocimiento del personal de la institución mediante las capacitaciones que se planteen considerando lo descrito en el numeral 3.17 del presente capítulo así como también al personal nuevo

que se incorpore a la institución independientemente del área o función para la que sea contratado.

Cuadro No. 11. Proceso general para la administración de R O.



Fuente: Autor del proyecto

Elaboración: Autor del Proyecto

3.6.1 Etapa de Identificación de los Factores de Riesgo operativo:

- **Objetivo**

Reconocer los factores de Riesgo a través de las fuentes internas de información que se cuenta en la Institución

- **Actores del Proceso**

Los actores de procesos son principalmente la Unidad de Riesgos, Auditoría Interna, Atención al Cliente, Oficial de Cumplimiento quienes por medio de sus informes y reportes proveen datos de mucha importancia para la generación de la base de eventos.

- **Descripción de la Actividad Número 1**

Los actores entregarán a la Unidad de Riesgos los reportes como insumo para la etapa de identificación de Factores de Riesgo.

- **Descripción de la Actividad Numero 2**

La Unidad de Riesgos realizará la Recopilación y Sistematización de Factores de Riesgo, procedimiento detallado en el Anexo 1 de este documento.

3.6.2 Etapa de Medición de los Factores de Riesgo.

- **Objetivo**

Realizar la ponderación y dimensionamiento de los diferentes factores de riesgo identificados dentro de todas y cada una de las actividades de la Mutualista Imbabura.

- **Actores del Proceso**

El actor principal de este proceso es la Unidad Integral de Riesgos de la institución bajo la responsabilidad del oficial de Riesgos y está bajo el control y la revisión del Comité Integral de Riesgos.

- **Descripción de la Actividad Número 1**

Se realizará la ponderación y priorización Previa de los Factores de Riesgo, en donde se utilizará tablas de severidad, tabla de frecuencia, tabla del nivel de Riesgo.

- **Descripción de la Actividad Número 2**

Se realizará la revisión de la Ponderación y Priorización elaborada en la actividad anterior.

- **Descripción de la Actividad Número 3**

Una vez revisada la Ponderación y Priorización posteriormente se aprueba los factores críticos

3.6.3 Etapa de Control/Mitigamiento de Riesgos operativos

- **Objetivo**

Establecer Planes de Acción, políticas y límites que permitan disminuir o eliminar los riesgos.

- **Actores del Proceso**

Los actores principales del proceso son: Dueños del Proceso, Operativos del Proceso, Auditoría Interna.

- **Descripción de la Actividad Número 1**

Una vez definidos los factores de Riesgos se prosigue a determinar los planes de acción para cada uno de ellos.

- **Descripción de la Actividad Número 2**

Se realizará el seguimiento al Plan de Acción establecido para mitigar el riesgo al que haga referencia, el mismo que pasará por cada actor del proceso para su observación.

3.6.4 Etapa de Monitoreo de Riesgos.

- **Objetivo**

Advertir señales de alerta a los actores y miembros del CAIR, sobre el nivel de riesgo actualmente administrado

- **Actores del Proceso**

Los actores principales del proceso son: Oficial de Cumplimiento, Auditoría Interna, Atención al Cliente.

- **Descripción de la Actividad Número 1**

La última fase de todo el Proceso de Administración de Riesgo Operativo es ya la evaluación de los factores de Riesgo Mitigados, fase final del proceso de administración el Riesgo Operativo, e inicio de la etapa nuevamente de ponderación y medición de los factores de Riesgo.

Cada una de las etapas del Proceso de Administración del Riesgo Operativo conlleva procedimientos y actores en el proceso de acuerdo a cada una de las etapas establecidas por tal razón es necesario desarrollar y documentar los procedimientos específicos para la aplicación de métodos de administración de riesgo operativo tal como se menciona a continuación.

3.7 GESTIÓN METODOLÓGICA Y PROCEDIMIENTOS ESPECÍFICOS DE RIESGO OPERATIVO.

La gestión de los riesgos operativos en la Mutualista Imbabura debe ser considerada como una práctica integral. A continuación se detalla un marco adecuado para la gestión del riesgo mediante la identificación, evaluación, seguimiento y control, adicionando además la función de la divulgación de información y capacitación de los funcionarios involucrados.

El manejo del Riesgo Operativo involucra la gestión eficiente de los mecanismos de control con una adecuada estructura en la institución que optimice las operaciones de la organización.

Los pilares fundamentales de la gestión operacional dentro de la institución son principalmente: procedimientos claros de operación, recurso humano calificado, un adecuado soporte tecnológico y de seguridad para el desarrollo de las operaciones, el manejo y control de las situaciones externas a la organización

El enfoque de gestión de riesgos se realizará bajo un esquema de análisis de la organización funcional de la Mutualista dividiéndola en los siguientes niveles:

- Junta General de Asociados,

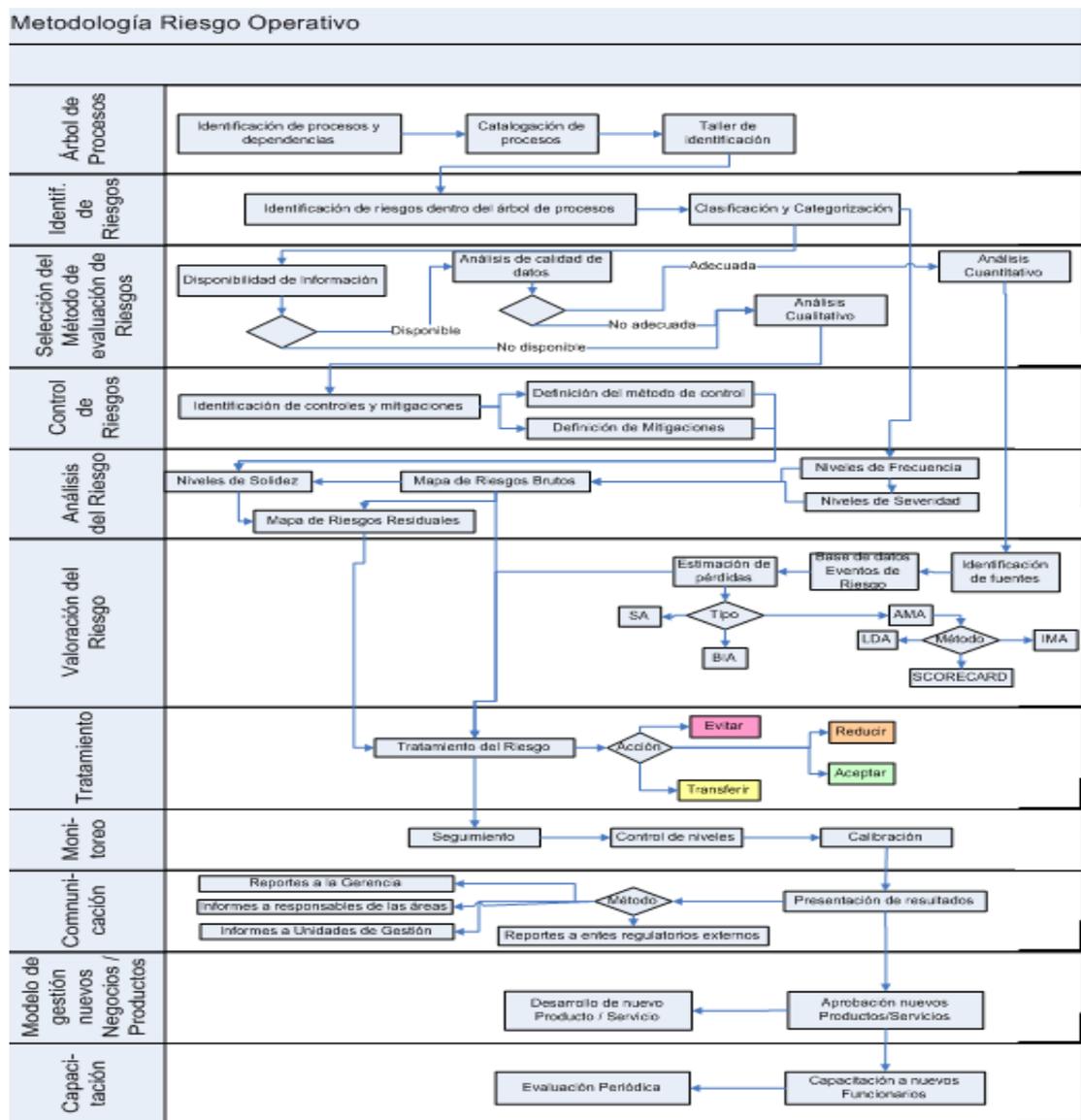
- Directorio,
- Comités,
- Gerente General,
- Sucursales y Agencias,
- Unidades operativas,
- Áreas comerciales.

El grado de compromiso y participación del Directorio, Gerencia General y demás funcionarios de la Mutualista Imbabura. En todo momento debe identificar y administrarse más eficientemente los riesgos que se desea asumir en base a la observación de los siguientes elementos.

- Definición de líneas de negocios, macroprocesos y procesos estableciendo sus metas, objetivos y alcances.
- Definición específica de las responsabilidades de las áreas que participan en la administración de los riesgos.
- Determinación de las relaciones entre las líneas de negocios, macroprocesos y procesos y las diferentes partes de la estructura de la organización.
- Dependiendo de las circunstancias, el análisis de los riesgos operativos puede realizarse en forma cualitativa, cuantitativa o una combinación de ambas.

A continuación se describe la metodología y los respectivos procedimientos específicos mediante los cuales se administran los diferentes riesgos operativos detectados en las actividades de la Mutualista Imbabura y la exposición externa que se genera de manera inherente.

Cuadro No. 12. Proceso específicos para la administración de R O.



Fuente: Documentos entregables

Elaboración: Grapo Context.

3.8 ÁRBOL DE PROCESOS.

El primer paso de administración de riesgos consiste en identificar los procesos sobre los cuales habrá que buscar indicios potenciales de riesgo, o en general pérdida de ingresos.

Para ello pueden utilizarse distintos métodos:

- Cuestionarios
- Entrevistas
- Flujogramas
- Organigramas

Análisis crítico propio de la información en función a los riesgos posibles.

Esta revisión incluye los manuales de organización y funciones de políticas y procedimientos.

Se ejecutará en una primera etapa por medio de reuniones programadas con dinámica orientada a talleres participativos, los que se complementarán con otros métodos de recolección de información con el fin de entender mejor los procesos, al contrastar datos o documentos relevados o proporcionados por los supervisores de cada área con usuarios operativos.

3.8.1 Identificación.

Para una mejor estructuración de los procesos que abarcan las funciones de la Mutualista Imbabura se ha decidido establecer su calificación en:

Líneas de Negocio: Las cuales representan a un producto o la generación de una línea de productos institucionales.

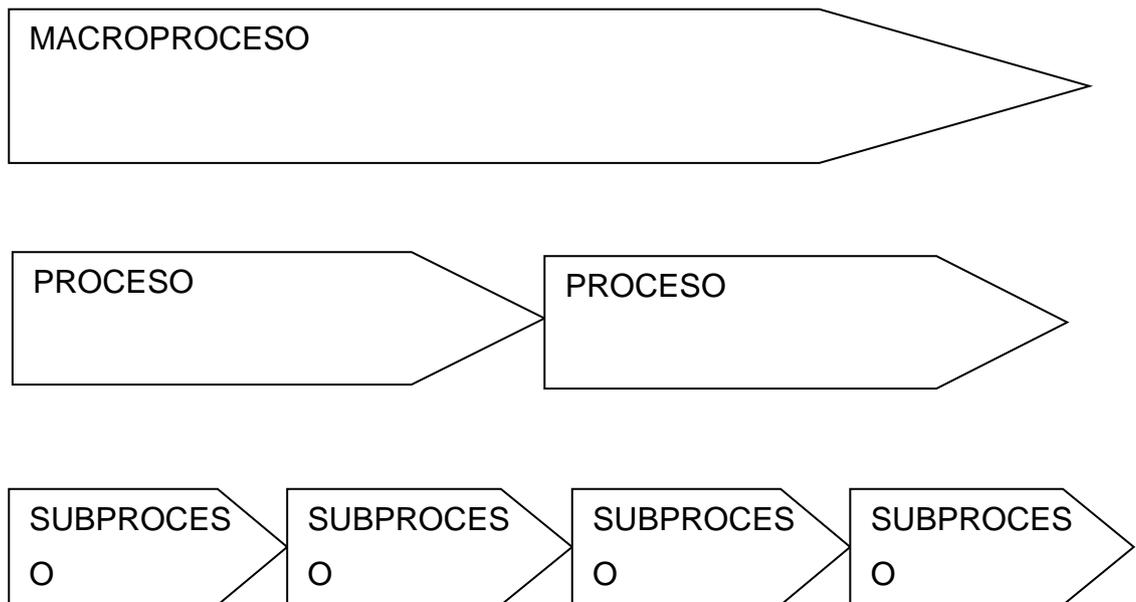
Macroprocesos: Cada línea de negocio se compone de macroprocesos los cuales constituyen un grupo de procesos afines.

Procesos: Constituyen un conjunto de procedimientos mediante los cuales se norma una ejecución determinada.

Subproceso: Grupo de actividades parciales que conforman un proceso

De este modo podemos concluir en un árbol de procesos que se ejemplifica según el siguiente gráfico:

GRAFICO No. 13 Árbol de procesos.



Fuente: Cadena de valor Mapa de Procedos

Elaboración: Corporación Lideres

Mutualista Imbabura ha tomado la totalidad de la actividad de la organización incluida dentro de la línea Banca Minorista, líneas de negocio del informe de Convergencia internacional de medidas y normas de capital emitido por el Comité de Supervisión Bancaria de Basilea.

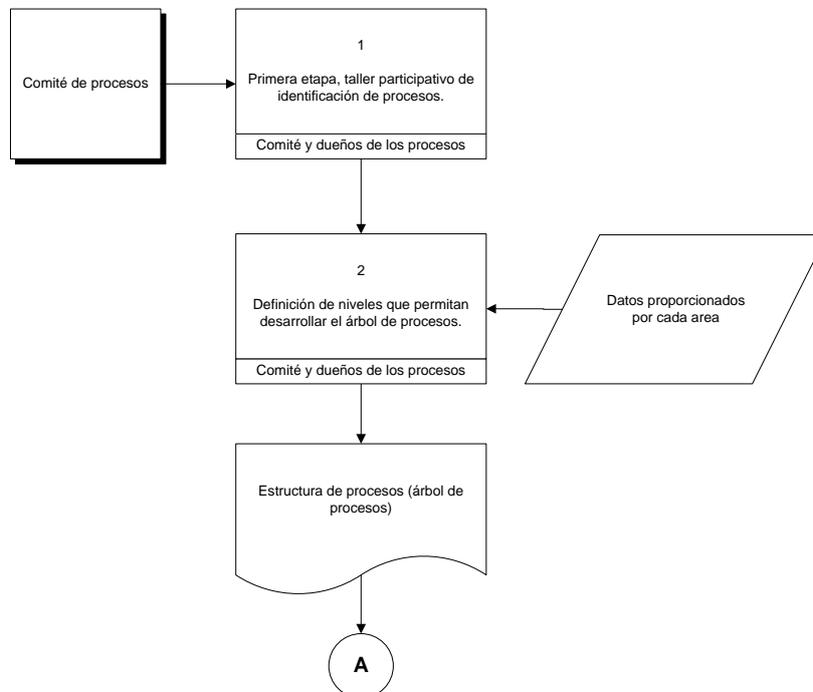
3.8.2 Catalogación.

Cabe agregar que para una mejor identificación, los procesos pueden catalogarse dentro de tres tipos diferentes:

- **Productivos:** Relacionados con la generación de productos/Servicios
- **De apoyo:** Sirven de soporte a los procesos productivos y complementan la toma de decisiones.
- **Estratégicos:** Sirven para tomar decisiones y están en manos de analistas expertos.

3.8.3 Procedimiento.

Cuadro No. 14. Procedimiento árbol de procesos



Fuente: Autor del proyecto

Elaboración: Autor del proyecto

Se ejecutará en una primera etapa por medio de una reunión programada bajo la modalidad de un taller participativo por parte de un comité denominado de procesos, durante el cual se establecerá una primera identificación de procesos.

De esta forma, el mencionado taller, permitirá que los principales funcionarios de Mutualista Imbabura definan los niveles de procesos que permitan desarrollar el esquema principal del árbol de procesos de la organización.

Los datos obtenidos podrán complementarse posteriormente con otros métodos de recolección de información con el fin de entender mejor los procesos, al contrastar datos o documentos relevados o proporcionados por los responsables de cada área con los usuarios de los sectores operativos. Posteriormente se agruparán de modo tal que el resultado final, represente la estructura de procesos de Mutualista Imbabura, agrupada en macroprocesos por Líneas de Negocio:

La Línea de Negocio Financiero contiene los siguientes macroprocesos:

- Cartera de crédito
- Ahorros a la Vista y Plazo Fijo
- Tesorería
- Servicios
- Otros Servicios
- Administración Informática
- Marketing
- Administrativo
- Administración Financiera Contable
- Control
- Administración de Riesgos

La Línea de Negocio Inmobiliario contiene los siguientes macroprocesos:

- Producción Inmobiliaria
- Compra de Terrenos
- Inmobiliarios

Un macroproceso se compondrá de procesos definidos según lo identificado en el comité de procesos que permitirá agrupar subprocesos claramente definidos (los identificados por los funcionarios en el taller inicial), constituyendo estas la base sobre las cuales se identificarán los riesgos. Cada uno de estos subprocesos será asociada con el sector responsable de su ejecución.

3.8.4 Documentación.

Se documentará el trabajo realizado de la siguiente forma:

- Se elaborará un cuadro resumen con el resultado del taller sobre la base de la información respondida por los funcionarios.
- Se obtendrá un árbol de macroprocesos de la organización con la totalidad de la información recabada.

3.9 IDENTIFICACIÓN DE RIESGOS.

La identificación de los riesgos operativos se realiza a través del relevamiento de información de las áreas responsables de los diferentes procesos la cual tendrá como finalidad dejar registrado para cada proceso enunciado, la siguiente información:

- Los riesgos operativos que se identifican en cada área y la clasificación de dicho riesgo para cada uno.
- Los controles existentes, la enunciación de los que en su opinión deben implementarse de manera adicional o sustitutiva, así como los responsables del control.
- Los eventos de riesgo que se hayan presentado para cada uno de los riesgos identificados.

3.9.1 Clasificación de Factores de Riesgo Operativo.

Se define como riesgo la probabilidad de que un suceso ocurra y provoque pérdidas a una persona individual o jurídica.

Los aspectos que originan los riesgos de operación han sido clasificados en cuatro grupos: de personas, de procesos, de tecnología y eventos externos.

3.9.2 Tipos de Eventos.

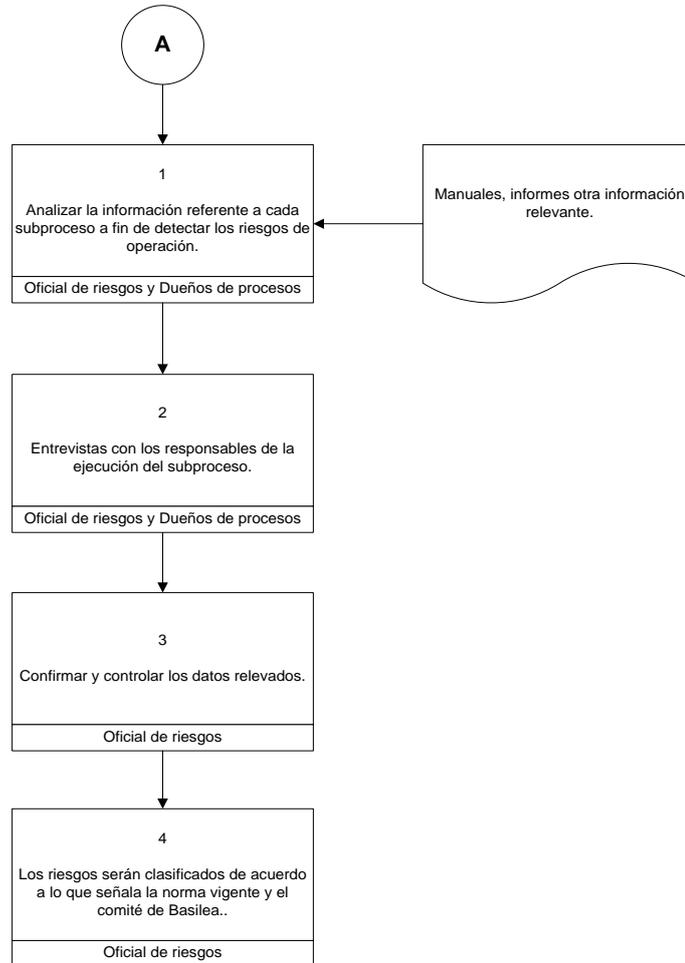
A los fines de la aplicación de una metodología que respete la clasificación realizada por el Comité de Basilea, se tendrán en cuenta la “Categorización de los eventos de riesgo del acuerdo de capitales de BASILEA II” que establece la siguiente categorización primaria de tipos de eventos:

- Fraude interno.
- Fraude externo.
- Relaciones laborales y seguridad en el puesto de trabajo.
- Clientes, productos y prácticas empresariales.
- Daños a activos materiales.
- Incidencias en el negocio y fallos en los sistemas.

- Ejecución, entrega y gestión de procesos

3.9.3 Procedimiento.

Cuadro No. 15. Procedimiento identificación de riesgos



Fuente: Autor del proyecto

Elaboración: Autor del proyecto

Una vez definida la estructura del árbol de procesos se analizará la información referente a cada subproceso a fin de detectar los riesgos de operación que pudieran contener:

- Manuales de procedimiento

- Informes de auditoría
- Otra documentación relevante

Entrevistas con los responsables de la ejecución del subproceso, supervisores y otros cuyas funciones puedan tener conexión con el mismo.

En razón de tratarse de opiniones que pueden estar influidas por un cierto grado de subjetividad, por realizarse con personas involucradas en la gestión de los subprocesos, se recomienda recabar información de más de una fuente a efectos de poder cruzar la misma y contar con la posibilidad de realizar un control por oposición de los datos relevados.

3.9.4 Documentación.

A los efectos de permitir la documentación de la totalidad de los riesgos detectados en las tareas de relevamiento de información se procederá al mapeo de los mismos en forma ordenada, clasificándolos según los procesos identificados, para lo cual:

- Se utilizará el mismo esquema de árbol de procesos.
- Sobre la base del árbol de procesos definido se confeccionará una planilla por cada subproceso identificado, incluyendo en forma ordenada, el detalle de actividades dentro del mismo y la categorización de la actividad.
- De este modo cada riesgo relevado se irá asociando a la actividad correspondiente dentro del subproceso, realizando una breve descripción del mismo a efectos de su individualización.

- Se indicará además el tipo de evento al que pertenece el riesgo.

3.10 SELECCIÓN DEL MÉTODO DE ANÁLISIS PARA LA EVALUACIÓN DE RIESGOS.

3.10.1 Disponibilidad de la información.

Para seleccionar el método más idóneo que permita realizar posteriormente un análisis de los riesgos identificados, se deberá verificar la información existente para cada uno de los riesgos o eventos que ya se han presentado dentro de la institución. En los casos donde se hayan identificado riesgos operativos o eventos pero aún no se disponga de información para su análisis histórico (frecuencia y severidad), la valoración de los riesgos corresponderá al método cualitativo o cuantitativo descrito posteriormente en el punto tipos de análisis que a continuación se describe.

3.10.2 Análisis de calidad de datos.

La calidad de la información es indispensable para poder cuantificar las pérdidas por efectos de la exposición a los diferentes riesgos.

Para analizar la calidad de datos entregados es importante verificar que las pérdidas provocadas por efecto de ocurrencia del riesgo o evento se encuentren disponibles y que hayan existido niveles previos de aprobación que hayan certificado el ingreso de dichos eventos de riesgo a una herramienta informática para proceder con el cálculo correspondiente.

Si los datos almacenados en la base de eventos de la herramienta informática son altamente confiables en cuanto a forma de registro y procedencia confiable, es posible utilizar métodos avanzados para la

valoración del riesgo previo consulta y puesta a conocimiento del organismo de control.

3.10.3 Tipos de análisis.

El análisis de los riesgos puede ser realizado con distintos grados de valoración, dependiendo esta de la información y datos a disposición.

El análisis puede ser cualitativo o cuantitativo. En la práctica, se recomienda iniciar con un análisis cualitativo para obtener una indicación general del nivel de riesgo.

En segunda instancia, una vez que la organización haya desarrollado sus mecanismos de recolección de información, será posible llevar a cabo un análisis cuantitativo más específico.

El detalle de los tipos de análisis que se pueden utilizar en riesgo operativo es el siguiente:

- **Análisis cualitativo:** El análisis cualitativo utiliza formatos descriptivos para identificar la magnitud potencial del evento y la probabilidad de ocurrencia del mismo.

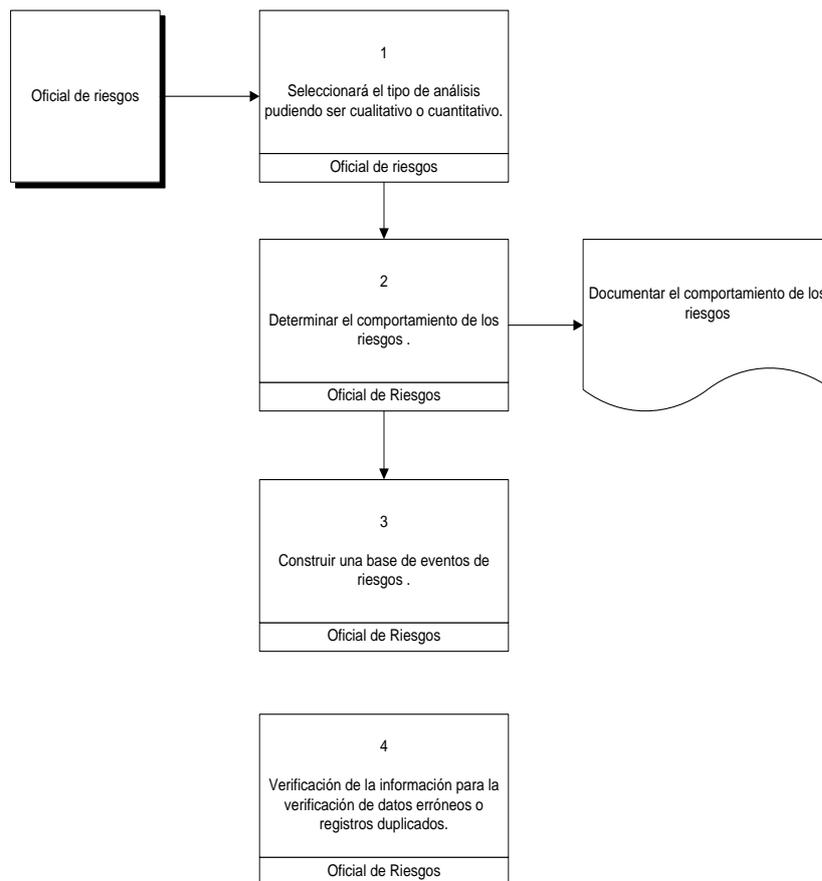
El análisis cualitativo se utiliza como una actividad inicial, para identificar los riesgos que posteriormente requerirán un análisis más detallado o cuando los datos numéricos son inadecuados para un análisis cuantitativo.

- **Análisis cuantitativo:** El análisis cuantitativo utiliza valores numéricos para los importes y probabilidades (en lugar de las escalas descriptivas utilizadas en los análisis cualitativos).

Utilizan datos de distintas fuentes y la calidad del análisis depende de la precisión e integridad de los valores numéricos recolectados.

3.10.4 Procedimiento.

Cuadro No. 16. Procedimiento para el análisis de riesgos



Fuente: Autor del proyecto

Elaboración: Autor del proyecto

En ésta etapa, se seleccionará el análisis cualitativo para la identificación del nivel de los riesgos. Este tipo de análisis permitirá determinar el comportamiento de los riesgos y documentarlos. Para efectuar análisis cuantitativos es necesario construir una base de eventos de riesgo y

garantizar a través de procesos automatizados, que la calidad de la información sea verificada y posea niveles de autorización para control de datos erróneos o registros duplicados.

3.10.5 Documentación.

Se incluirá en la documentación, la selección del tipo de análisis a utilizar para la ejecución del proceso de análisis de riesgos o valoración del riesgo.

3.11 CONTROL DEL RIESGO.

Son las políticas y procedimientos que se implementan para ayudar a asegurar que las respuestas a los riesgos se llevan a cabo eficazmente. Los tipos de actividades de control pueden ser diversos, incluyen controles preventivos, detectivos, manuales, computarizados, gerenciales. Incluyen una gama de actividades tales como aprobaciones, autorizaciones, verificaciones, conciliaciones, revisiones de funcionamiento, seguridad de activos y la segregación de funciones.

Las actividades del control son aplicadas con respecto a cada uno de las cuatro categorías de objetivos: estratégicos, de operaciones, de información y de cumplimiento.

La Unidad de Riesgos deberá considerar las actividades existentes de control asegurándose que las mismas sean suficientes y asegurándose que estén ejecutadas con eficacia.

Las actividades de control deben ser ejecutadas a través de la totalidad de la organización por todos los niveles de su estructura y en cada una de las funciones que se realicen. Con el propósito de identificar los controles establecidos para minimizar los riesgos es necesario conocer el componente en más detalle.

Las actividades de control en Mutualista Imbabura comprenden:

- Evaluación del diseño de los procesos elaborados por los responsables de los controles.
- Identificación de controles claves.
- Evaluación de controles generales y de aplicación de tecnología de la información.
- Pruebas para comprobar la efectividad de los controles claves

3.11.1 Controles.

El proceso de control se inicia a través de un levantamiento de los procesos operativos durante el cual se debe centrar la atención en aquellos controles que minimizan los factores de riesgo ya identificados.

El primer paso consiste en identificar los controles generales, que se aplican ayudan a asegurar la continuidad de los procesos analizados.

A continuación se deberán proceder a la revisión de los controles operativos, que incluyen pasos automatizados que hacen a la utilización de herramientas tecnológicas.

Estos, se combinan además con otros controles de procesos manuales, en algunos casos necesarios, que aseguran el cumplimiento y la exactitud y validez de la información.

La evaluación de los elementos de control permite su calificación y permite minimizar la probabilidad de ocurrencia de los riesgos asociados.

A los efectos de la planificación, la calificación del control o del conjunto de controles está relacionada directamente con su riesgo asociado.

3.11.2 Métodos de control.

El riesgo operativo puede ser minimizado sobre la base de controles internos y externos. A modo de ejemplo, se enumeran a continuación algunos controles habitualmente utilizados.

Los métodos de controles internos consisten en:

- **Separación de funciones:** los responsables de las transacciones no deberían tener funciones de liquidación Y contabilización.
- **Entradas duales:** los inputs deberían ser controlados a través de dos fuentes diferentes, esto es, el comprobante de la operación y la confirmación de la misma por parte de un back office.
- **Conciliaciones:** los resultados deberían ser controlados a través de diferentes fuentes.
- **Sistemas de aviso:** fechas importantes deberían ser ingresadas dentro de un sistema de calendarios que generen alertas automáticamente.

Son métodos de controles externos, entre otros:

- **Confirmaciones:** el comprobante de la operación necesita ser confirmado con su contraparte, hecho que permite un chequeo independiente de la transacción.

- **Verificación de precios** (para el caso de tener que valuar posiciones): los precios deberían obtenerse de fuentes externas confiables.
- **Autorizaciones:** los sectores involucrados deberían estar provistos de la lista de las personas autorizadas a negociar como así también de una lista de transacciones permitidas.
- **Liquidación:** el proceso de pago en sí mismo puede indicar si alguno de los términos de la transacción ha sido correctamente registrado.
- **Auditorias:** Los exámenes proveen importante información sobre las áreas con debilidades potenciales en la estructura organizacional.

La solidez del conjunto de controles implementados representa la valoración cualitativa del mismo.

3.11.3 Mitigaciones.

Representan acciones tomadas con relación a los riesgos detectados que permiten reducir el impacto de estos sobre las actividades de la organización.

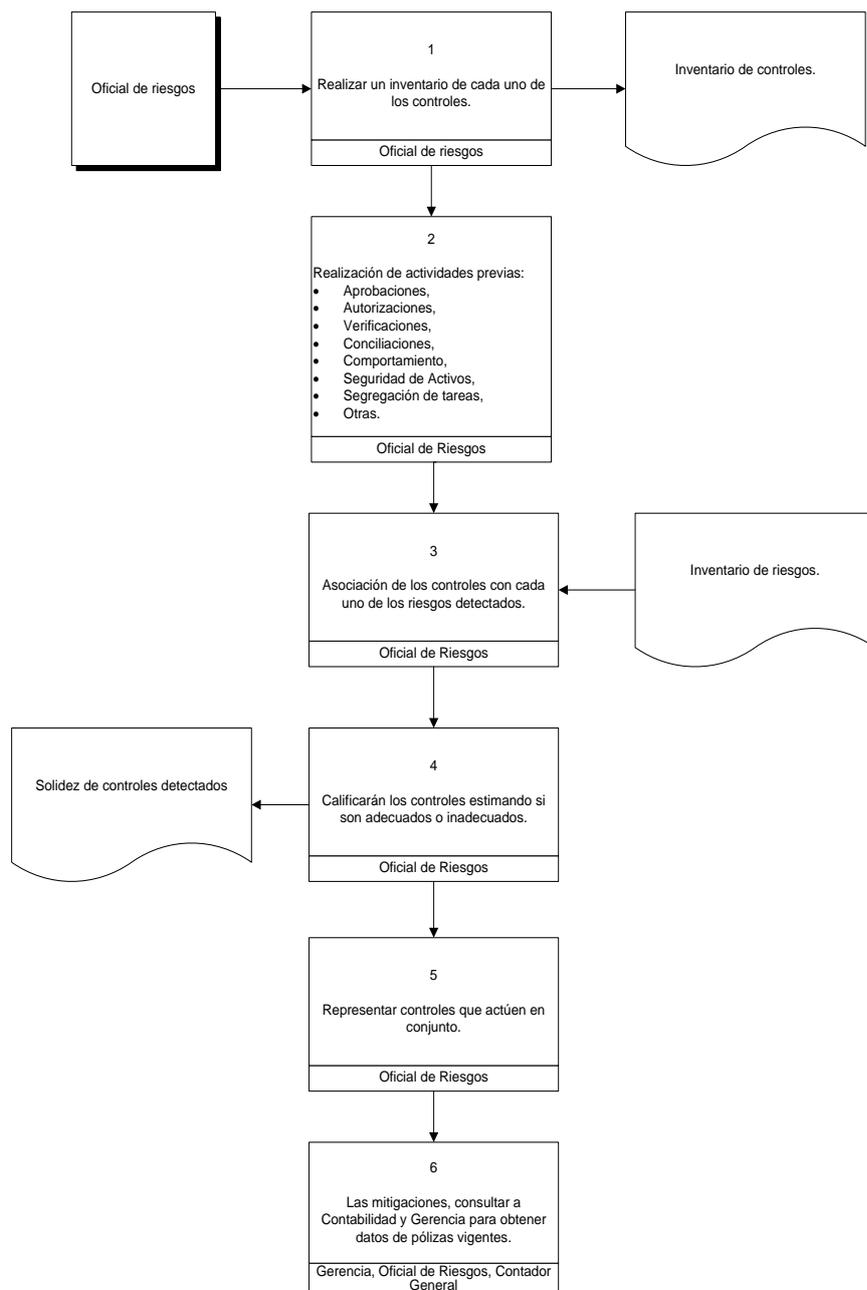
Las mitigaciones devienen de la contratación de seguros cuya cobertura posibilita la reducción del efecto cuantitativo de la ocurrencia de un evento de riesgo. A efectos de su incorporación al esquema de valoración cuantitativa, se debe tener en cuenta con respecto a cada mitigación relevada los siguientes factores:

- **Costo anual:** Es el costo anual del contrato de seguro.

- **Valor deducible:** Es el monto no cubierto por la compañía aseguradora en caso de producirse el siniestro.
- **Límite asegurado por evento:** Es el importe establecido en la póliza que representa el límite máximo de indemnización a percibir.

3.11.4 Procedimiento.

Cuadro No. 17. Procedimiento de control de riesgos



Fuente: Autor del proyecto

Elaboración: Autor del proyecto

En primer lugar se realizará un inventario de todos y cada uno de los controles, para lo cual se recurrirá en primera instancia a los mismos procedimientos utilizados para identificar los riesgos.

A tal efecto se analizará una serie de actividades tales como:

- Aprobaciones

- Autorizaciones
- Verificaciones
- Conciliaciones
- Comportamiento operacional
- Seguridad de activos
- Segregación de tareas
- Otras.

Como resultado de las tareas deberán hallarse los controles existentes y asociarlos a cada riesgo detectado.

Como paso siguiente se calificarán dichos controles estimando si los mismos son adecuados e intentando determinar la eficiencia de los mismos de modo tal que pueda proyectarse una idea aproximada de la solidez de los mismos. Cabe agregar que deberán analizarse en grupo aquellos controles que actúen en forma conjunta sobre un riesgo determinado, representando un conjunto de controles.

Para el caso de las mitigaciones corresponderá consultar con el área contable y de administración a efectos de obtener los datos correspondientes a las pólizas de seguros vigentes contratados por la institución en resguardo de sus activos.

3.11.5 Documentación.

El documento mediante el cual se levanta la planilla para el relevamiento de mitigaciones se la realiza considerando como mínimo la siguiente información: actividad, riesgo, descripción del riesgo, mitigación, tipo, costo anual, valor deducible, valor cobertura y solidez. La solidez deberá estar dentro de un rango adecuado o inadecuado.

3.12 ANÁLISIS DEL RIESGO.

Una vez realizado el levantamiento de información por parte de las áreas responsables, la misma será remitida a la Unidad de Riesgos, la cual, realizará una evaluación preliminar de los datos informados y consolidará los resultados, evaluará lo descrito y emitirá opinión sobre la exposición al riesgo que registra la organización sobre la base de los resultados obtenidos.

Las dos herramientas fundamentales para el análisis de riesgos son:

- **Mapa de Riesgos Brutos:** se define como una herramienta metodológica que permite hacer un inventario de los riesgos en forma ordenada y sistemática, organizándolos para una evaluación en función de su probabilidad de ocurrencia e impacto económico para la organización.
- **Mapa de Riesgos Residuales:** El Mapa de Riesgos Residuales contiene el resultado final de la exposición al riesgo de los procesos de la organización una vez identificados los controles y acciones mitigadoras que actúan a fin de corregir la ocurrencia y severidad de los riesgos brutos. Del análisis del mapa de riesgos residuales se pueden inferir las características de la exposición al riesgo de la organización.

Los factores fundamentales para obtener el Mapa de Riesgos Brutos y el Mapa de Riesgos Residuales son: la probabilidad de ocurrencia, severidad o impacto económico a la organización y solidez de los controles y acciones mitigadoras que se aplican para reducir la probabilidad de ocurrencia y/o el impacto económico.

A continuación se describen estos conceptos y su aplicación en el Mapa de Riesgos Brutos y el Mapa de Riesgos Residuales:

3.12.1 Probabilidad de ocurrencia.

Para determinar la probabilidad de ocurrencia de eventos con un horizonte determinado, se utiliza una distribución de conteo que explicita la probabilidad de ocurrencia de una determinada cantidad de eventos para dicho horizonte a partir de la población expuesta, es decir, de las pérdidas registradas por la entidad.

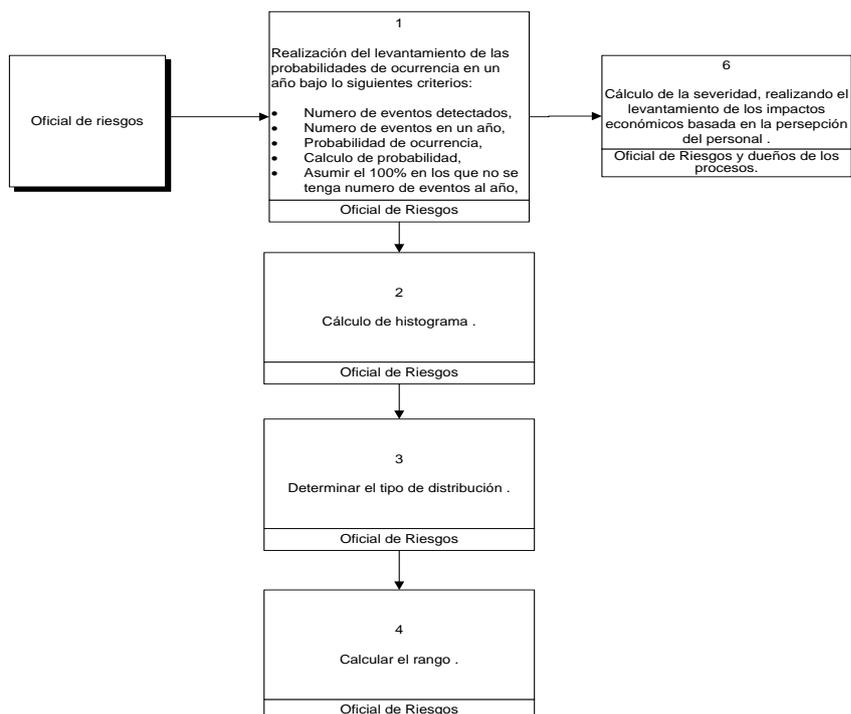
La distribución seleccionada es aquella que, dadas sus características, permite establecer de forma apropiada el número de eventos a partir de la media de la frecuencia de eventos observada en el pasado.

Hasta tanto no se cuente con la recolección de la información necesaria para establecer la probabilidad de ocurrencia en forma cuantitativa, la misma será evaluada cualitativamente de acuerdo a la evaluación de los sectores involucrados.

La probabilidad de ocurrencia, deberá expresarse en un número anual de ocurrencias.

3.12.2 Procedimiento.

Cuadro No. 18. Procedimiento de análisis riesgos



Fuente: Autor del proyecto

Elaboración: Autor del proyecto

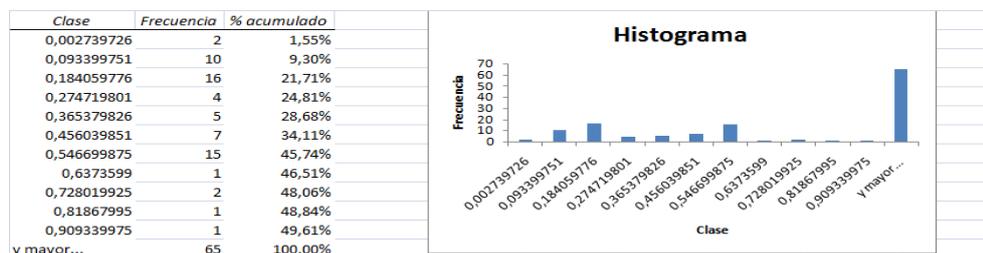
Se realiza el levantamiento de las probabilidades de ocurrencia o número de veces de ocurrencia de los eventos de riesgo operativo en un año, tomando en cuenta los siguientes criterios:

- Recopilación sobre el número total de eventos (No. Total de Eventos).
- Levantamiento sobre el número de ocurrencias del evento de riesgo que podrían suceder en el año (No. Eventos que podrían ocurrir).
- El levantamiento de información de probabilidad de ocurrencias se basa en la información disponible por la Mutualista y la percepción del personal interviniente en los diferentes procesos identificados.
- Seguidamente se realiza el cálculo de la probabilidad de ocurrencia estandarizada: $\text{No. Eventos que podrían ocurrir} / \text{No. Total de Observaciones}$.

- En los casos en los cuales no se disponga de información sobre el número total de observaciones (No. Total de Eventos), se asumirá el 100 % es decir 1,00 para el valor de la probabilidad de ocurrencia estandarizada.

Una vez que se han calculado las probabilidades de ocurrencias estandarizadas, se procede a calcular el histograma mediante el cual se estimarán las categorías de distribución de ocurrencias sobre los datos de probabilidad de ocurrencia estandarizada. Para la estimación del histograma se considera una distribución de las categorías de rangos con una longitud de clase de acuerdo al porcentaje acumulado de probabilidades de ocurrencias con respecto al total.

CUADRO No 19. Ejemplo de Histograma



Fuente: Sistema Finanware

Elaboración: Grupo Context

Los resultados de la estimación del histograma establecen el número de clases en que es necesario distribuir los datos. Sin embargo, de ser el número de clases un valor alto, procede realizar una distribución más homogénea para lo cual se usa el siguiente procedimiento para ajustar el número de clases:

- De los datos estandarizados, se calcula el máximo y el mínimo.

- Con ambos datos, se calcula el rango estadístico (máximo menos mínimo).
- Una vez estimado el rango estadístico, se divide para el número de clases requerido, con lo cual se obtiene el tamaño de las clases a estimar.

Una vez estimada la longitud de clase, se procede al cálculo de los rangos, tal y como se muestra a continuación:

- Límite inferior + tamaño de clase = límite superior
- Límite Superior (Rango 1) + tamaño de clase = Límite Superior (Rango 2)
- Y así sucesivamente hasta completar el límite superior indicado.

Un ejemplo de los cálculos se indica a continuación:

CUADRO No 20. Ejemplo de cálculo

Valor máximo	1,00000	
Valor mínimo	0,00274	
Rango estadístico	0,99726	
No. clases	5	
Tamaño clases	0,19945205	
	Inferior	Superior
Clase 1	0	0,20219
Clase 2	0,20219	0,40164
Clase 3	0,40164	0,60110
Clase 4	0,60110	0,80055
Clase 5	0,80055	1,00000

Fuente: Sistema Finanware

Elaboración: Grupo Context

Según lo anterior una probable clasificación de probabilidades de ocurrencia se indica a continuación:

- Muy Alta: El evento muy probablemente ocurrirá en forma continua
- Alta: El evento probablemente ocurrirá en varias ocasiones

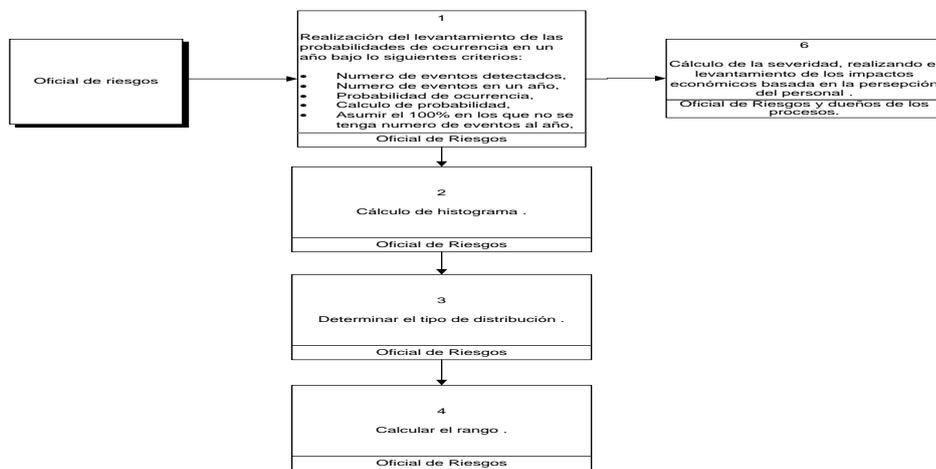
- Media: El evento puede ocurrir en algunas ocasiones
- Baja: El evento puede ocurrir eventualmente
- Muy Baja: El evento puede ocurrir en algún momento y es poco probable que suceda.

3.12.3 Severidad.

Una vez estimada la distribución de frecuencias se debe proceder a estimar la distribución del monto de pérdida (severidad o impacto) de los eventos. En virtud de eso es necesario estudiar la base de pérdidas operativas para ajustar la distribución que mejor se adecue a los datos observados de montos de pérdidas. La severidad monetaria debe estar expresada en la moneda en curso legal (Dólar americano).

3.12.4 Procedimiento.

Cuadro No. 21. Procedimiento de Análisis de riesgos



Fuente: Autor del proyecto

Elaboración: Autor del proyecto

Se realiza el levantamiento de las severidades o impactos económicos que puede ocasionar la ocurrencia de un evento de riesgo operativo. Esta información se basa en la percepción del personal interviniente en los diferentes procesos identificados.

Para la determinación de las categorías de severidad, se utilizará la regla de Sturge, la cual, permite relacionar la longitud de la clase con respecto al rango estadístico, de acuerdo a la siguiente fórmula:

$$S = \frac{X - y}{1 + (3,22 * \text{Log}_{10}(N))}$$

Donde:

S = regla de Sturge

X = límite superior

y = límite inferior

N = número total de severidades

Una vez estimada la longitud de clase, se procede al cálculo de los rangos, tal y como se muestra a continuación:

- Límite inferior + S = Límite Superior (Rango 1)
- Límite Superior (Rango 1) + S = Límite Superior (Rango 2)
- Y así sucesivamente hasta completar el límite superior de la muestra.

Un ejemplo de los cálculos se indica a continuación:

CUADRO No 22. Ejemplo de cálculo.

Valor máximo	1.400.000,00
Valor mínimo	0,00000
Rango estadístico	1400000,00000
N	126
Longitud	7,763193155
Tamaño clase	180338,164

Fuente: Sistema Finanware

Elaboración: Grupo Context

Los resultados de la estimación indican que es necesario distribuir los datos en 8 clases. Sin embargo, en base a una distribución más homogénea se usa el siguiente procedimiento para ajustar el número de clases:

De los datos estandarizados, calcular el máximo y el mínimo.

Con ambos datos, se calcula el rango estadístico (máximo menos mínimo)

Una vez estimado el rango estadístico, se divide para el número de clases requerido, con lo cual se obtiene el tamaño de las clases a estimar.

Una vez estimada la longitud de clase, se procede al cálculo de los rangos, tal y como se muestra a continuación:

- Límite inferior + tamaño de clase = límite superior.
- Límite Superior (Rango 1) + tamaño de clase = Límite Superior (Rango 2).
- Y así sucesivamente hasta completar el límite superior indicado.

Los cálculos se indican a continuación:

CUADRO No 23. Ejemplo de cálculo.

Valor máximo	1400000,00000
Valor mínimo	0,00000
Rango estadístico	1400000,00000
No. clases	5
Tamaño clases	280000

Fuente: Sistema Finanware

Elaboración: Grupo Context

Según lo anterior una probable clasificación de severidades se indica a continuación:

- **Severo:** Se registran daños significativos que se producen por una pérdida en la capacidad de operación. Existen pérdidas financieras altas.
- **Muy Importante:** Existen daños y perjuicios que en ocasiones solo pueden ser solucionados con la asistencia de un tercero. Hay pérdidas financieras muy importantes.
- **Importante:** Existen daños y perjuicios considerables. Hay pérdidas financieras importantes.
- **Medio:** Los daños o perjuicios pueden ser subsanados en forma inmediata. Existen pérdidas financieras medias.
- **Bajo:** Hay daños o perjuicios menores. La pérdida financiera es menor.

3.12.5 Solidez de los controles.

Una vez estimada la probabilidad de ocurrencia y severidad de los riesgos, se identifican los controles y acciones mitigadoras existentes para determinar cómo esos controles y acciones mitigadoras apoyan a una eficiente gestión de riesgo operativo. El parámetro de medición de los controles y acciones mitigadoras se denomina solidez.

Para determinar la solidez los controles, éstos se evalúan conforme a dos factores:

3.12.6 Diseño.

Adecuado: Corresponde a controles cuya implementación haya sido valorada previamente en otras experiencias internas o externas como adecuado para realizar seguimiento y verificación y que además cuente con un procedimiento manual o automático para su ejecución.

Inadecuado: Corresponde a controles de los cuales no haya sido verificado su resultado en experiencias previas o haya sido valorado como insuficiente o como solución temporal para seguimiento y control, hasta la implementación de un procedimiento manual o automático.

3.12.6.1 Eficiencia.

- **Alta:** El control implementado responde efectivamente al control de los riesgos.
- **Media:** El control ofrece resultados parciales y debe ser complementado con la ayuda de otros procedimientos y controles.
- **Baja:** El control no ha demostrado eficiencia o se desconoce el resultado que se puede obtener con su implementación.

De este modo, la combinación de los dos factores precedentes permite que un control o un conjunto de controles pueden clasificarse de acuerdo a su solidez en:

- **Sólido:** Control probado previamente en la institución que permite reducir probabilidad de ocurrencia y severidad, definido únicamente como de diseño adecuado y eficiencia alta.
- **Adecuado:** Control de fácil implementación y validación de resultados, que no haya sido probado previamente en la institución o su resultado no haya sido susceptible de medición. Puede ser definido como diseño adecuado y eficiencia media, diseño adecuado y eficiencia alta, diseño adecuado y eficiencia baja, y diseño inadecuado y eficiencia media.
- **Normal:** Control susceptible de implementación y validación de resultados, que no haya sido probado previamente en la institución o su resultado no haya sido susceptible de medición. Puede ser definido como diseño adecuado y eficiencia Alta, diseño adecuado y eficiencia media, y todos los tipos de diseño inadecuado.
- **Inadecuado:** Control cuyos resultados de implementación sean inciertos. Puede ser definido como diseño adecuado y eficiencia baja, y todos los tipos de diseño inadecuado.

3.12.7 Mapa de riesgos brutos.

El diseño de un Mapa de Riesgos Brutos facilita la visualización y la comprensión de los riesgos que se le presentan a la entidad en los distintos niveles de su operación (líneas de negocio, macroprocesos, procesos, subprocesos), facilitando la definición de las medidas de respuesta o tratamiento.

El Mapa de Riesgos Brutos clasifica a los riesgos en términos de la probabilidad de ocurrencia de los eventos y la severidad económica que representan.

Los riesgos identificados para cada proceso o componente del mismo deben ser calificados. Para este procedimiento se tienen en cuenta ciertos criterios que servirán como base para determinar su valoración.

La configuración del Mapa de Riesgos Brutos, considera los rangos de probabilidad de ocurrencia y rangos de severidad indicados anteriormente, y su combinación establece la calificación de riesgo bruto. Esta calificación es definida también en rangos que representan el nivel de riesgo para la organización.

La calificación de riesgo bruto se califica en cuatro niveles según la incidencia que presente respecto del proceso analizado. Los niveles son:

- **Extremo:** Requiere atención inmediata. Debe ser Tratado como “Evitar”.
- **Alto:** Necesita atención a nivel gerencial. Debe ser Tratado como “Reducir”.
- **Medio:** Debe especificarse una responsabilidad para su atención. Debe ser Tratado como “Transferir”.
- **Bajo:** Se administra mediante procedimientos de rutina. Debe ser Tratado como “Aceptar”.

Tanto los rangos de probabilidad de ocurrencia, de severidad como de calificación de riesgo bruto deberán ser ajustados periódicamente con el objetivo de tener una adecuada distribución del riesgo.

A continuación se indica el modelo de un Mapa de Riesgos Brutos:

GRAFICO No. 24. Mapa de riesgos brutos.

		Severidad				
		Severo	Muy Import	Importante	Medio	Bajo
Frecuencia	Muy Alta	Extremo	Extremo	Extremo	Alto	Medio
	Alta	Extremo	Extremo	Alto	Medio	Bajo
	Media	Extremo	Alto	Medio	Medio	Bajo
	Baja	Alto	Medio	Medio	Bajo	Bajo
	Muy Baja	Medio	Bajo	Bajo	Bajo	Bajo

Fuente: Documentación de Sistema Finanware

Elaboración: Grupo Context.

3.12.8 Mapa de riesgos residuales.

Para configurar una Mapa de Riesgos Residuales, se definen rangos de la solidez de los controles asociados a los riesgos y la combinación con las calificaciones de riesgo bruto establecidas en el Mapa de Riesgos Brutos, define la calificación de riesgo residual.

Esta calificación es definida también en rangos que representan el nivel de riesgo para la organización. La calificación de riesgo residual se califica en cuatro niveles según la incidencia que presente respecto del proceso analizado (ver Anexo 2). Los niveles son cuatro:

- **Riesgo Residual Extremo:** Requiere atención inmediata. Debe ser Tratado como “Evitar”.

- **Riesgo Residual Alto:** Necesita atención a nivel gerencial. Debe ser Tratado como “Reducir”.
- **Riesgo Residual Medio:** Debe especificarse una responsabilidad para su atención. Debe ser Tratado como “Transferir”.
- **Riesgo Residual Bajo:** Se administra mediante procedimientos de rutina. Debe ser Tratado como “Aceptar”.

Tanto los rangos de solidez de los controles, como de calificación de riesgo residual deberán ser ajustados periódicamente con el objetivo de tener una adecuada distribución del riesgo. La Solidez de los controles se establece a través de una relación entre la eficiencia probada del control y la calidad del diseño del mismo. Bajo las definiciones de Diseño y Eficiencia, se ha elaborado una matriz que permite establecer la solidez de los controles y/o acciones mitigadoras:

GRAFICO No. 25. Matriz de controles

		Diseño	
		Adecuado	Inadecuado
Eficiencia	Alta	Sólido	Adecuado
	Media	Adecuado	Normal
	Baja	Inadecuado	Inadecuado

Fuente: Documentación de Sistema Finaware

Elaboración: Grupo Context

De acuerdo a la relación directa entre la eficiencia y el diseño de los controles, se determina la solidez de los mismos. El valor de solidez se

utilizará dentro del mapa de riesgos residuales para identificar la afectación al riesgo bruto, de la implementación de controles.

A continuación se indica el Mapa de Riesgos Residual:

GRAFICO No. 26. Mapa de riesgos residual

		Solidez de los Controles			
		Inadecuado	Normal	Adecuado	Sólido
Riesgo Bruto	Extremo	Extremo	Extremo	Alto	Alto
	Alto	Extremo	Alto	Alto	Medio
	Medio	Alto	Medio	Medio	Bajo
	Bajo	Medio	Medio	Bajo	Bajo

Fuente: Documentación de Sistema Finaware

Elaboración: Grupo Context

Una vez obtenidos los resultados serán puestos a conocimiento del comité integral de riesgos y deberá constar en el acta de la reunión en la que se trata el tema previa aprobación del directorio de la Mutualista Imbabura.

3.13 VALORACIÓN DEL RIESGO

3.13.1 Valoración cuantitativa.

Con la finalidad de presentar un modelo de continuidad a las tareas de Gestión de los Riesgos Operativos dentro de Mutualista Imbabura, se detallan a continuación los criterios generales para una valoración cuantitativa de los eventos y seguidamente un esquema de registro de una base de eventos y pérdidas, estos podrán variar de acuerdo a la implementación de herramientas de medición de riesgo operativo.

3.13.1.1 Cuantificación de las pérdidas.

Un evento de Riesgo Operativo es un incidente que ocasiona que el resultado de un proceso de negocio difiera del resultado esperado, debido a fallas en los procesos internos, las personas, los sistemas o por eventos externos, y por lo tanto genera un riesgo de pérdida.

Las pérdidas deberán cuantificarse como el importe necesario para retrotraer la situación de la entidad financiera al momento previo a la ocurrencia del evento, considerando los siguientes criterios:

- En caso que la pérdida involucre algún bien con valor de mercado conocido, se deberá tener en cuenta este último, más los gastos adicionales que correspondan.
- Si se trata de una pérdida contingente, se tendrá en cuenta el monto de la previsión registrada contablemente.
- No sólo deben ser contempladas aquellas erogaciones que queden reflejadas en el cuadro de resultados, sino también aquellas que se activen contablemente (por ejemplo, el reemplazo de un equipo total o parcialmente amortizado);
- En el caso de los costos indirectos, si pueden ser subsanados internamente sin incurrir en un gasto adicional, no deberían ser incluidos. Si se debe incurrir en un gasto extraordinario, deberán ser incluidos.

Hay ocasiones en las cuales el impacto de un evento por Riesgo Operativo está reflejado a través de provisiones. Esto ocurre frecuentemente en el contexto de situaciones litigiosas o en eventos complejos que requieren un mayor tiempo para ser investigados o remediados.

Se deberá reportar la previsión (actualizándola de ser necesario) cuando la misma afecte unívocamente al evento.

En los casos en los cuales un mismo evento causara simultáneamente impactos positivos y negativos, se deberán compensar entre sí y registrarse sólo si el resultado neto resulta negativo.

3.13.1.2 Base de datos de eventos y pérdidas.

La base de datos representa una necesidad en el desarrollo de un modelo de cuantificación. Una base de datos conteniendo pérdidas operativas históricas requiere la alimentación fundamental del modelo de cuantificación de riesgo operativo y es lo que permitirá el traspaso de un enfoque cualitativo a un enfoque integral.

La mencionada base de datos se deberá desarrollar a partir de un proceso homogéneo de recolección de pérdidas y de asignación de éstas en función de las distintas áreas y de los diferentes tipos de riesgos, no sólo con el fin de registrar las pérdidas, sino también para entender sus causas.

Se deberán incluir todos aquellos eventos que, siendo cuantificables, hayan generado pérdidas o hayan sido provisionados contablemente y también se deberán informar las cuasi-pérdidas, entendiéndose por tales, a los eventos operativos que no resultan en una pérdida financiera.

Los siguientes ítems asociados a eventos de Riesgo Operativo, entre otros, deberían ser incluidos a efectos de determinar el monto asociado al evento:

- Cargos a resultados.
- Pérdidas de mercado.
- Costos de reparación o reemplazo para restituir el bien a la situación original.
- Honorarios pagados a abogados externos.

En cambio se excluirán:

- Costos de oportunidad
- Eventos que causen pérdidas por riesgo reputacional.
- Eventos que causen pérdidas por riesgo estratégico.

En un principio se registrarán la totalidad de los eventos antes descritos, sin establecerse un umbral mínimo para el monto de las pérdidas. El objetivo es disponer de información que permita evaluar si en un futuro resulta conveniente la adopción de tal umbral, que cumpla con los objetivos de establecer un límite al volumen de información registrada y, simultáneamente, evitar filtrar datos que pudiesen ser necesarios para la gestión correcta del riesgo.

Los eventos repetidos, originados por la misma causa –por ejemplo, repetidos por el mismo agente o debidos a un mismo plan de acción- deberán registrarse como incidentes separados.

Un evento de carácter operacional que afecte también a otro tipo de riesgos (crédito o mercado) deberá igualmente registrarse en la base de Riesgo Operativo cuando la principal causa de la pérdida sea un evento de naturaleza operacional, debiendo especificarse el vínculo con el otro riesgo.

3.13.1.3 Base de datos mínima.

A efectos de implementar el correspondiente registro de los eventos de riesgo operativo cuantificables, se establece que los registros deberán incluir los siguientes campos:

- **Identificación:** los eventos de pérdida operativa deberán ser identificados de manera secuencial y unívoca.

- **Fecha de inicio estimada.**
- **Fecha de finalización.**
- **Fecha de registro contable** (de corresponder).
- **Fecha de descubrimiento:** Los eventos por RO deberán ser incorporados a la base en la fecha de su descubrimiento.
- **Descripción:** deberá asentarse una descripción del evento, fundamentalmente los factores desencadenantes o causas que le dieron origen. El grado de detalle de la información descriptiva será directamente proporcional a la severidad del mismo.
- **Tipo de evento:** se clasificará al evento en alguna de las categorías ya establecidas por el Comité de Basilea.
- **Línea de negocio:** los importes deberán ser imputados en alguna de las líneas de negocio de Mutualista Imbabura.
- **Área responsable:** se consignará el área en la que se produjo la pérdida, En caso de que el evento de pérdida haya sucedido en una unidad centralizada o en una actividad que incluya más de una línea de negocio, se deberá distribuir el importe de la pérdida a pro rata, utilizándose para ello una base razonable, fundada y verificable.
- **Proceso:** se informará el proceso al que está vinculado el evento de Riesgo Operativo.
- **Monto:** Se imputará el monto siguiendo los criterios generales y las bases de valuación / medición citados previamente.

- **Cuenta contable:** Se identificará, en caso que parte o el total del monto haya sido imputado contablemente, la cuenta contable en la que se imputó dicho monto.
- **Cobertura con pólizas de seguro:** se deberá consignar el porcentaje cubierto por una póliza de seguros, en caso que esto sea pertinente.

3.13.2 Métodos de cuantificación.

Convergencia Internacional de Medidas y Normas de Capital emitido por el Comité de Supervisión Bancaria de Basilea propone tres métodos de cálculo para los cálculos de requerimientos de capital por riesgos operativos:

- Básico (BIA)
- Estándar (SA)
- Modelos avanzados (AMA)

Son tres enfoques de complejidad creciente, cuyo propósito es permitir que las entidades se desplacen a entornos más precisos y sofisticados de medición y gestión del riesgo operacional.

3.14 TRATAMIENTO DEL RIESGO

3.14.1 Planteo general.

El tratamiento de los riesgos identificados involucra las posibles respuestas que pueden implementarse; el análisis de dichas opciones, las cuales no necesariamente son mutuamente excluyentes, incluye la posibilidad de:

- **Evitarlos:** La acción es tomada para evitar afrontar los riesgos inclusive evitando ejecutar las actividades que pueden provocarlos.

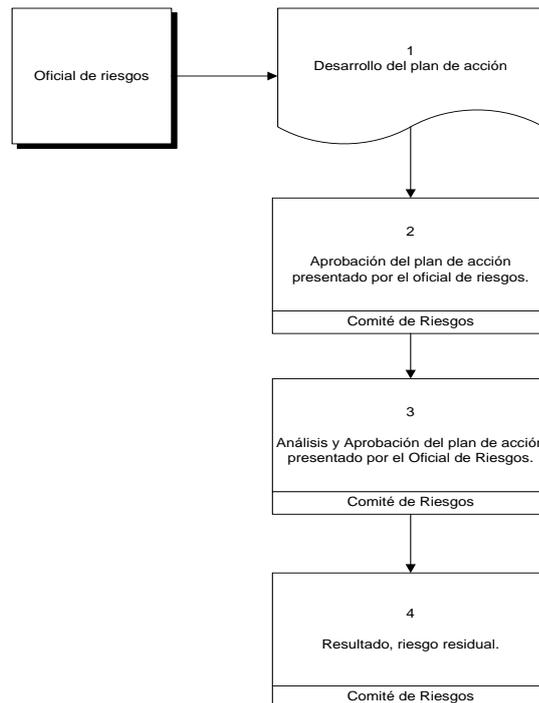
Puede no realizarse una expansión comercial a un nuevo ámbito geográfico o mercado. Evitar un riesgo significa que el costo sobre los mismos excede los beneficios deseados, o que no se encuentra una respuesta que permita reducir el impacto a un nivel aceptable. De todos modos debe tenerse en cuenta que en ocasiones evitar inadecuadamente algunos riesgos puede provocar un aumento significativo de la ocurrencia de otros.

- **Reducirlos:** La acción se toma para reducir la probabilidad de ocurrencia, el impacto o ambos. Corresponde generalmente a la toma de decisiones respecto de actividades comerciales. Reducir un riesgo significa llevarlo a límites de tolerancia admitidos en la política fijada por la dirección de la organización.
- **Transferirlos:** La acción es utilizada para reducir el impacto transfiriendo una porción del riesgo involucrado. Comprende técnicas de seguros o tercerización de actividades.
- **Aceptarlos:** No se toma ninguna acción que afecte la probabilidad de ocurrencia o el impacto. Ocurre en los casos en que se determina que el costo a incurrir en el intento de reducción es superior al generado por el propio riesgo.

Estas opciones deben ser evaluadas teniendo en cuenta el alcance de la reducción del riesgo y los niveles de aceptabilidad se corresponderán con los criterios operativos, técnicos, legales u otros, de acuerdo con las políticas, metas y objetivos internos de la organización. La opción más apropiada involucra balancear los costos de implementación contra los beneficios derivados de la misma razón por la cual se requiere de la valoración de los riesgos.

3.14.2 Procedimiento.

Cuadro No. 27. Procedimiento de tratamiento de riesgos.



Fuente: Autor del proyecto

Elaboración: Autor del proyecto

El procedimiento comprende un Plan de acción, que deberá ser trazado por la Unidad de Riesgos y elevado al Comité Integral de Riesgos para su aprobación. Se analizarán los efectos del riesgo y se identificarán diversas alternativas de tratamiento del riesgo, es decir de acciones o respuestas posibles para su gestión. Se deberá proponer al Comité de Riesgos el desarrollo de la combinación de tratamientos más apropiada para cada riesgo en función de los resultados de su evaluación, de forma que el riesgo detectado con anterioridad a la aplicación del tratamiento, pueda ser reducido a un nivel aceptable (riesgo residual). Incluye los siguientes pasos:

- **Prioridad de atención:** Una vez analizados los riesgos por proceso y subproceso, se resumen y se establece la prioridad de atención.
- **Acciones:** Se determinan qué acciones se deben implementar para mitigar el riesgo, en forma efectiva.

- Responsables: Se asigna un responsable del proceso y de la acción específica.
- Recursos: Se especifica en detalle los requerimientos para llevar a cabo la acción propuesta.
- Limitantes Se analizan los factores que pueden impedir el desarrollo de las acciones de mitigación.
- Plazos: Se debe fijar el cronograma de implementación de las acciones y la fecha de inicio de las mismas

3.14.3 Documentación.

El modelo básico de los planes de acción deberá por lo menos el compromiso de mejora, responsable, equipo de apoyo, presupuesto (de ser requerido) prioridad, fecha de inicio y fecha de fin.

Es imprescindible destacar que la documentación presentada al Comité Integral de Administración de Riesgos con los planes de tratamiento del riesgo, favorablemente aprobados, deberá obrar como documentación, formando parte de los papeles de trabajo de la Unidad de Riesgos, para una adecuada revisión del cumplimiento de las metas propuestas en el curso de los procedimientos mencionados.

3.15 MONITOREO.

El monitoreo constante es una parte integral del plan de tratamiento de la administración de riesgos. Los riesgos y la efectividad de las medidas de control necesitan ser monitoreadas para asegurar que no se registren

cambios que alteren las prioridades de los riesgos. A tal fin se deben considerar al menos para efectos de análisis:

- Las técnicas de medición adecuadas para el análisis requerido, que permitan identificar los supuestos y parámetros utilizados en dicha medición.
- Las técnicas de evaluación adecuadas para minimizar la posibilidad de pérdidas financieras relacionadas al diseño inapropiado de los procesos críticos
- Las políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.
- Asimismo, corresponderá controlar que no se afecten las probabilidades de ocurrencia y el impacto sobre los resultados, como también los factores que afectan la conveniencia o costos de las distintas opciones de tratamiento. En consecuencia, es necesario repetir regularmente el ciclo de administración de riesgos

3.15.1 Planteamiento general.

La Unidad de Riesgos deberá:

- Realizar un seguimiento periódico de los perfiles de riesgo y la exposición a situaciones de pérdida. De este modo se asegurará continuidad en los planes de acción definidos para los eventos de riesgo y se verificará que estos planes se cumplan con eficacia según lo establecido.

Dentro de la etapa de monitoreo se deberá:

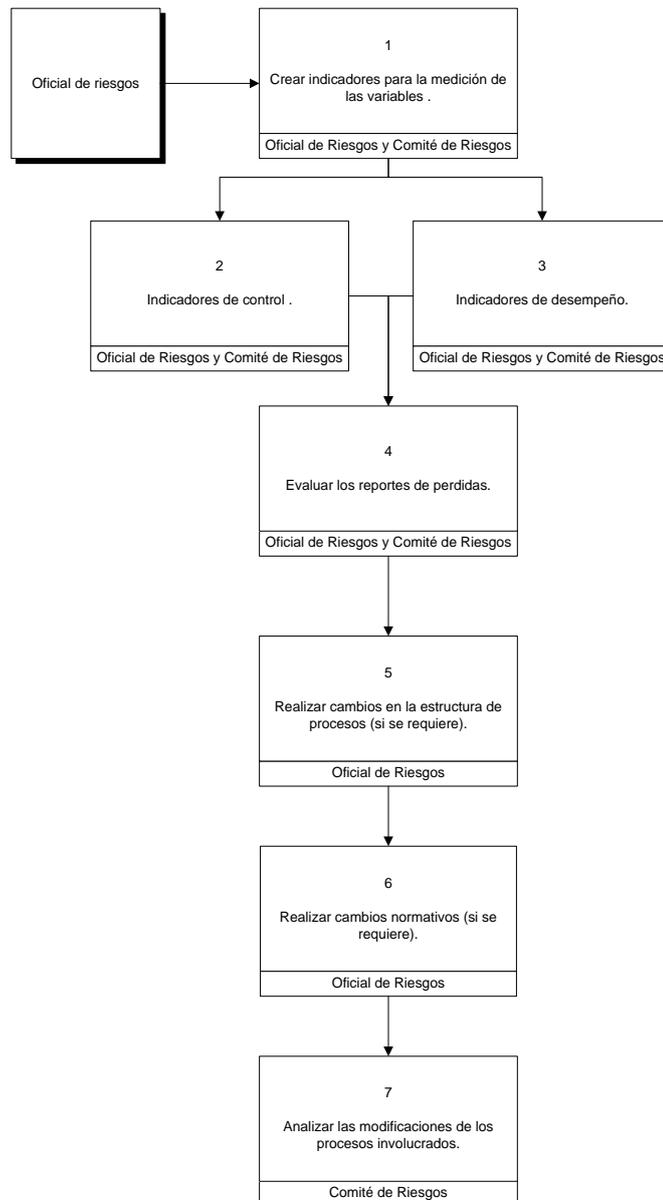
- Garantizar un monitoreo periódico del nivel de exposición al riesgo de la organización.

- Implementar un seguimiento efectivo que permita detectar y corregir las deficiencias encontradas.
- Realizar un seguimiento al comportamiento de los indicadores definidos.
- Verificar que los controles estén funcionando de forma oportuna y efectiva.
- Controlar que los riesgos residuales se encuentran en los niveles de aceptación establecidos por la organización.
- Evaluar la eficacia y el cumplimiento de los requisitos en el registro de eventos del riesgo operativo y verificar que se encuentre debidamente actualizado.
- Evaluar los procedimientos para el registro del riesgo operativo, analizando el impacto contable y económico que tienen dichos eventos para la organización.
- Realizar un seguimiento permanente respecto a los registros, procedimientos y posibles modificaciones que se generen en el proceso de implementación y puesta en marcha de la gestión de riesgos.
- Presentar informes periódicos sobre el funcionamiento y desarrollo de la gestión de riesgos, analizando de forma detallada cada hallazgo relevante, realizando de forma particular la respectiva recomendación.

- Evaluar que efectivamente se pongan en marcha los correctivos establecidos por la Unidad de Riesgo Operativo para la disminución de los eventos de riesgo operativo que se presenten

3.15.2 Procedimiento.

Cuadro No. 28. Procedimiento de Monitoreo de riesgos.



Fuente: Autor del proyecto

Elaboración: Autor del proyecto

Una vez identificados y evaluados los riesgos operativos, y propuestas las medidas de mitigación es necesario implementar las tareas de monitoreo mediante:

- Indicadores: Entendidos como la expresión cuantitativa del comportamiento de ciertas variables o de los atributos de un proceso determinado
- La magnitud del indicador al ser comparada con un nivel de referencia, podrá estar señalando una desviación o un acierto, sobre la cual se tomarán acciones correctivas o preventivas además de verificar el cumplimiento de las metas respecto del objetivo fijado. La medición se realiza través de la comparación una referencia frente a la cual confrontar el valor de un indicador
- Indicadores de control: cantidad de veces que se aplicó el control sobre cantidad de eventos de riesgo asociados detectados
- Indicadores de desempeño: Cantidad de eventos ocurridos sobre total de operaciones.
- Evaluación de reportes de pérdidas: Permite el análisis de los riesgos operativos por medio de una metodología cuantitativa. En la medida en que los presentes reportes se encuentren implementados, el análisis de los mismos permitirá evaluar la probabilidad de ocurrencia y el impacto de los riesgos detectados y conformará la base sobre la cual se podrán medir los indicadores de control para fijar las metas a cumplir.
- Cambios en la estructura de los procesos: Por medio de la revisión periódica de los procedimientos y la verificación del cumplimiento de los manuales que norman su puesta en práctica se deberá

analizar la respuesta que será necesaria implementar como consecuencia de las modificaciones implementadas.

- Lanzamiento nuevos productos y servicios.
- Cambios en el marco normativo: Verificando que las normas y procedimientos internos se correspondan con las modificaciones realizadas en leyes y documentación emitida por entes de supervisión.
- Se deberá analizar asimismo que las mencionadas modificaciones guarden el cumplimiento de la totalidad de las actividades de control respecto de la ejecución de los procesos involucrados.
- Cambios en la exposición al riesgo: Pueden producirse por situaciones propias de la dinámica de la gestión de la organización. Se verificará la necesidad de ajustar los procedimientos de control a efectos de que los mismos provean la reducción del riesgo a niveles aceptables con la estructura de la organización.

3.15.3 Documentación.

Los indicadores de control deberán hacer referencia al riesgo, al control implementado el indicador del control y la meta que se quiera cumplir o el porcentaje de cumplimiento. De la misma manera aplican para los modelos de indicadores de desempeño.

3.16 COMUNICACIÓN

Los resultados del análisis serán comunicados en forma oportuna a los niveles directivos y demás responsables de los procesos involucrados.

3.16.1 Sistemas de información y comunicación.

Comprende los procesos por medio de los cuales se genera y transmite información apropiada y oportuna a:

- Junta General de Asociados
- Directorio
- Comités
- Gerente General
- Sucursales y Agencias
- Jefaturas
- Resto del personal

Como así también a los interesados externos tales como:

- Entes de Control
- Organismos de Crédito
- Calificadoras de Riesgos

La organización deberá tener sistemas de información adecuados para medir, monitorear, controlar e informar sobre la gestión de los riesgos operativos. Estos sistemas deberán:

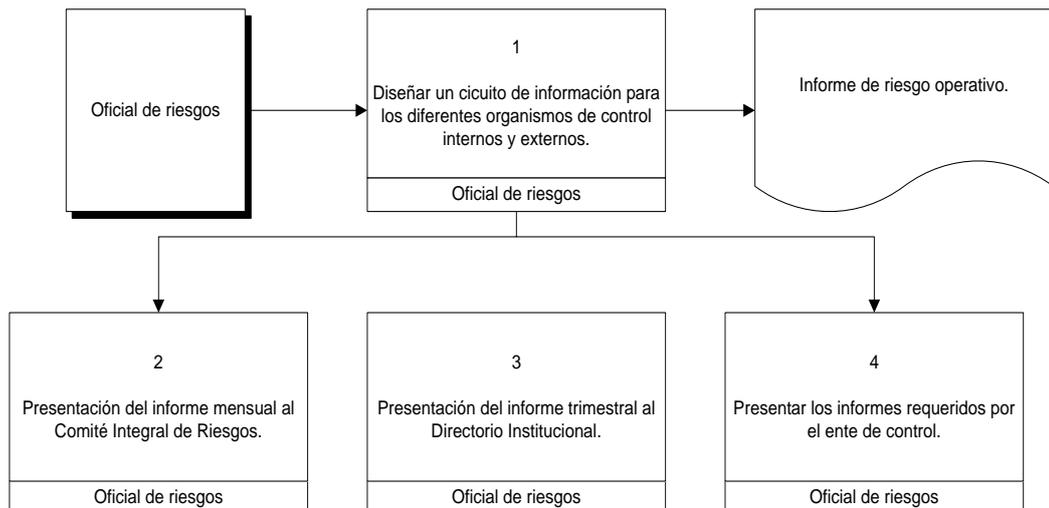
- Utilizarse para verificar el cumplimiento de las políticas, límites y procedimientos establecidos.
- Permitir evaluar la tendencia del grado de exposición de la organización al Riesgo Operativo.

- Proveer en forma oportuna informes necesarios al Comité Integral de Administración de Riesgo, Directorio Institucional, Organismos de Crédito e Inversionistas, Superintendencia de Bancos y Seguros, Calificadora de Riesgos para la toma de decisiones.
- Proveer los informes necesarios al resto del personal involucrado en la gestión del riesgo a los efectos de que los mismos cuenten con la información suficiente para el cumplimiento de sus funciones.

Resulta importante que la comunicación se realice en forma efectiva para asegurar que aquellos responsables de implementar la administración de riesgos comprendan los fundamentos de la toma de decisiones y las razones por las que se requieren ciertas acciones en particular.

3.16.2 Procedimiento.

Cuadro No. 29. Procedimiento de comunicación de información de riesgos.



Fuente: Autor del proyecto

Elaboración: Autor del proyecto

La Unidad de Riesgos es la encargada de diseñar un circuito de información que responda a los requerimientos de los diferentes interesados para el cumplimiento de sus funciones, de modo tal que los mismos se encuentren involucrados en el proceso de gestión de riesgos de la organización y deberá contemplar como mínimo:

- Presentación del informe mensual al Comité Integral de Administración de Riesgos para su conocimiento y aprobación correspondiente.
- Presentación del informe trimestral al Directorio Institucional para su conocimiento y aprobación correspondiente. Estos informes también podrán ser requeridos de acuerdo a la necesidad de la institución.
- Informes requeridos por entes externos (Superintendencia de Bancos y Seguros, Calificadora de Riesgos, entre otros).

3.17 MODELO DE GESTIÓN DE RIESGOS PARA NUEVOS NEGOCIOS Y PRODUCTOS

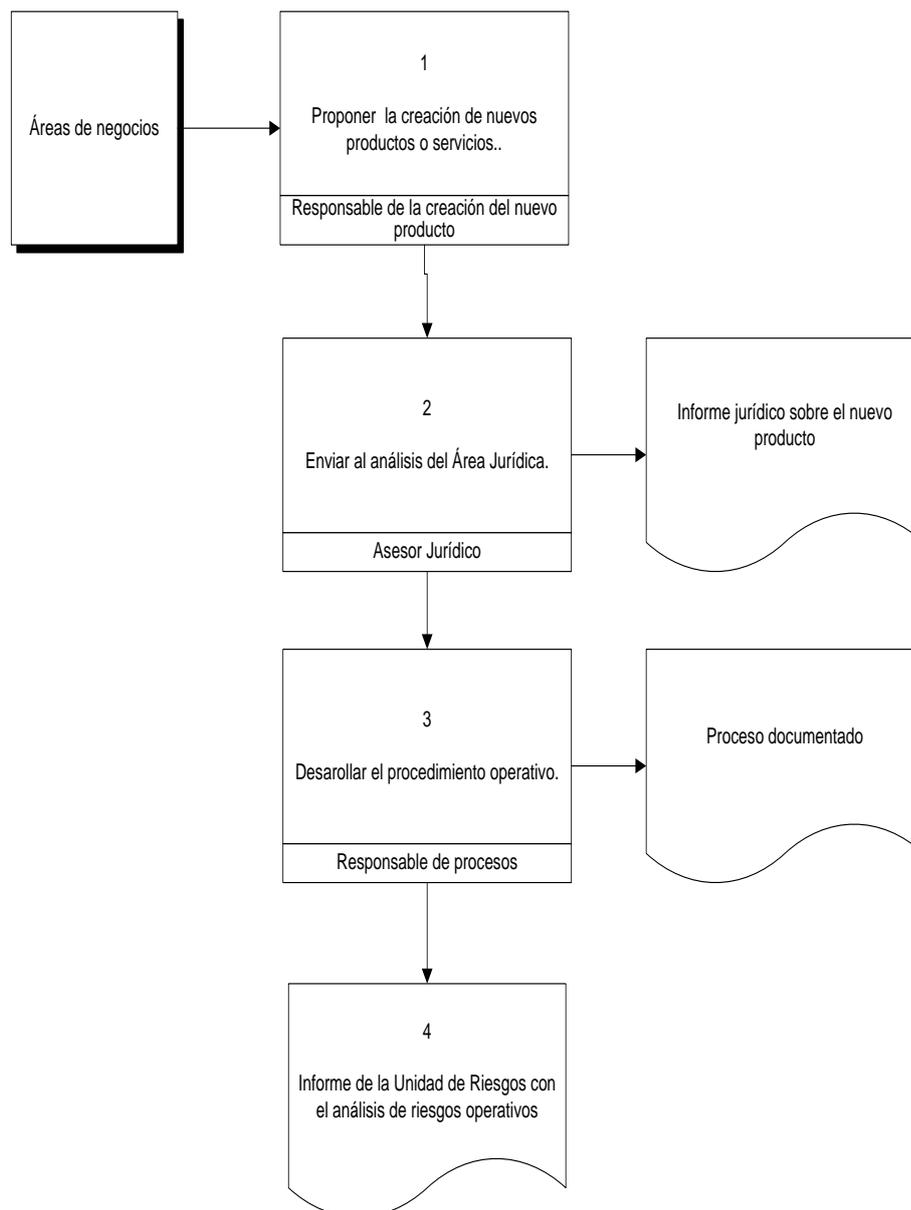
El proceso para la aprobación de propuestas de nuevas operaciones, productos y servicios que deberá contar, entre otros aspectos, como mínimo con una descripción general de las actividades de la nueva operación o el proceso propuesto, producto o servicio de que se trate, los riesgos identificados y las acciones a tomar para su control y el riesgo residual o inherente. El control no estará a cargo únicamente del Oficial de Riesgos sino también del Asesor jurídico quién emitirá un informe analizando la exposición al riesgo legal entre otras cosas.

Con el fin de controlar el riesgo de comenzar a operar en un nuevo producto o negocio, sin el debido conocimiento de la exposición que se genera para la

institución, se establecerá un procedimiento previo a cualquier operación en un nuevo producto o negocio.

3.17.1 Procedimiento.

Cuadro No. 30. Procedimiento de modelo de gestión para nuevos productos



Fuente: Autor del proyecto

Elaboración: Autor del proyecto

Los aspectos que se deberán tomar en cuenta en la creación de nuevos productos o servicios de la organización, incluyen:

- Análisis del Área Jurídica respecto del cumplimiento de las leyes y normativa vigente, dejando establecida la capacidad legal para operar el nuevo producto.
- Procedimiento operativo del nuevo producto y/o servicio.
- Requerimientos de tecnología, comunicaciones y desarrollo de sistemas.
- Informe de la Unidad de Riesgos con el análisis de los riesgos operativos, usando la metodología descrita en el presente manual.

3.17.2 Documentos de descargo.

El Comité de Riesgos elaborará para su elevación ante el Directorio Institucional un informe conteniendo toda la documentación sobre el análisis del nuevo producto o negocio a los efectos de obtener una decisión final respecto de su desarrollo.

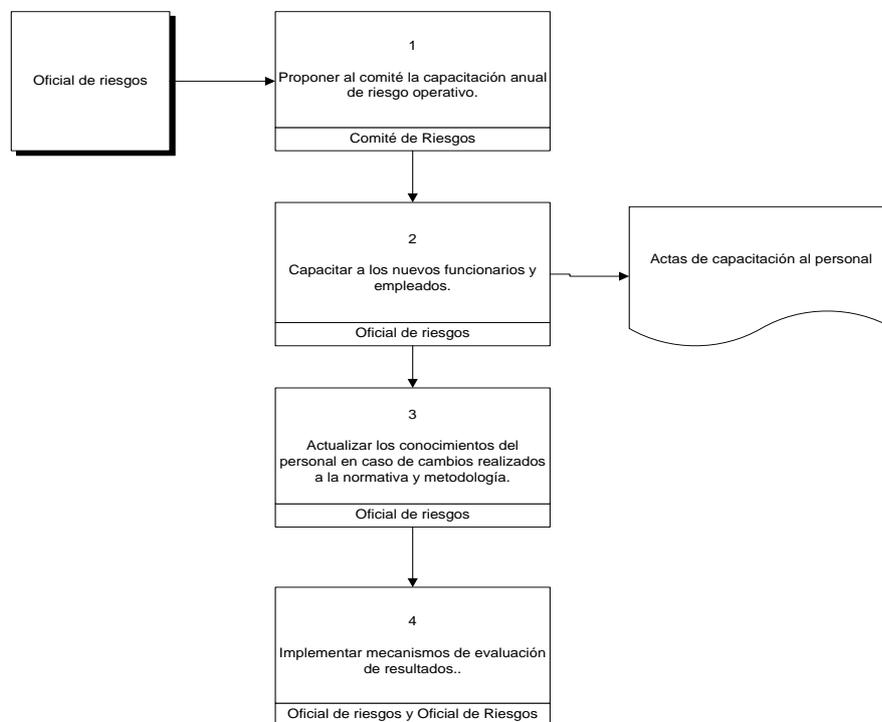
3.18 CAPACITACIÓN.

Se asigna a la Unidad de Riesgos la tarea de desarrollar y coordinar programas de capacitación para todas las áreas y funcionarios de la organización respecto del tratamiento de los riesgos operativos con una periodicidad anual o a su vez cuando el Comité Integral de Riesgos así lo considere previa autorización del Directorio de la entidad. En el proceso de inducción o capacitación al personal de la institución se explicará y se dará a conocer el proceso general de administración de riesgo operativo

Será responsable de proponer las actividades necesarias para asegurar que la información concerniente a los procedimientos de riesgo sea divulgada periódica y adecuadamente, llegando al conocimiento de todos los funcionarios, cuidando que estos permanezcan actualizados en cuanto al funcionamiento y requerimientos del Sistema.

3.18.1 Procedimiento.

Cuadro No. 31. Procedimiento de capacitación de riesgo operativo



Fuente: Autor del proyecto

Elaboración: Autor del proyecto

Los programas de capacitación a desarrollar considerarán los siguientes aspectos:

- Se planificarán con periodicidad anual teniendo en cuenta una adecuada distribución de los mismos atendiendo a las prioridades de los puestos con mayor requerimiento en razón de una mayor

exposición al riesgo y cuidando que al finalizar el período todo el personal se encuentre debidamente actualizado en la materia.

- Serán impartidos a los nuevos funcionarios y empleados que se incorporen a la organización.
- Estarán bajo un proceso de constante revisión y actualización.
- Se implementarán mecanismos de evaluación de los resultados obtenidos que permitan determinar el alcance de los objetivos propuestos.

3.18.2 Documentos de descargo.

Se generará las comunicaciones internas que correspondan a fin de informar a los funcionarios y resto del personal de la obligatoriedad de formar parte de los planes de capacitación previstos

Asimismo se presentará al Comité de Administración Integral de Riesgos en forma periódica la información correspondiente al avance de las tareas de capacitación en cumplimiento de los programas implementados

CAPITULO IV

4 ANÁLISIS DE IMPACTOS

En el presente capítulo se analiza los principales impactos que genera la implementación del Manual de Riesgo Operativo en Mutualista Imbabura logrando así establecer aspectos positivos y negativos de los mismos. Los impactos a analizar son: Impacto en procesos, impacto en Personas, impacto en tecnología de información e impacto en eventos externos; para lo cual, se utilizó una metodología basada en indicadores y niveles de valoración.

4.1 Bases teóricas.

Para cada tipo de impacto se ha establecido indicadores que fueron cuantificados por los principales actores del proyecto, la sumatoria de los datos totales de los descriptores, en los diferentes grados, divididos para el número de indicadores, permitió identificar el nivel de impacto de cada aspecto. Asimismo con los resultados de cada aspecto, considerado, se logró establecer el impacto global del proyecto. Con la finalidad de efectuar un análisis cuantitativo y cualitativo se ha elaborado una Matriz de Valoración, como se detalla a continuación:

CUADRO No 32. Cuantificación de impactos

INDICADOR	NIVEL DE IMPACTO						
	-3	-2	-1	0	1	2	3
TOTAL							
Nivel del Impacto							

Fuente: Propia

Elaboración: Autor del proyecto

Se puede observar en la matriz una valoración de –3 a 3, que se califica de acuerdo a los siguientes criterios:

CUADRO No 33 Matriz de valoración

PUNTAJE	SIGNIFICADO
-3	Impacto alto negativo
-2	Impacto medio negativo
-1	Impacto bajo negativo
0	Ni negativo, ni positivo
1	Impacto bajo positivo
2	Impacto medio positivo
3	Impacto alto positivo

Fuente: Propia

Elaboración: Autor del proyecto

El indicador se constituye por cada uno de los criterios que se aplican con la finalidad de realizar el análisis de cada impacto.

Para conocer el grado de impacto se emplea la siguiente ecuación:

$$NI = \frac{\sum \text{grado} \rightarrow \text{impacto.}}{n^{\circ} \text{ indicadores}}$$

4.2 IDENTIFICACIÓN DE LOS IMPACTOS.

4.2.1 Impacto en Procesos.

La implementación del Manual de Riesgo Operativo va a mejorar el manejo de los procesos mediante un análisis continuo de los mismos para mantener una adecuada actualización, esto favorece a la institución puesto que podría ser más competitivas con procesos ágiles que le

permitan ganar posicionamiento en el mercado. También organiza los métodos mediante los cuales se desarrollan las actividades evitando cuellos de botella que retrasen la consecución de los productos financieros

**CUADRO No 34.
MATRIZ DE IMPACTO EN PROCESOS**

INDICADOR	NIVEL DE IMPACTO						
	-3	-2	-1	0	1	2	3
Agilidad en concluir productos							X
Ventaja competitiva						X	
Crecimiento de colocación						X	
Captar más segmentos de mercado					X		
TOTAL					1	4	3

Fuente: Propia

Elaboración: Autor del proyecto

$$\text{Nivel de impacto} = \frac{1 + 4 + 3}{4} = 2,00$$

De acuerdo al análisis, el nivel de impacto en procesos es 2 positivo; la implementación de este proyecto dará agilidad a la colocación de créditos y busca un mejor posicionamiento de mercado mediante la implementación de procesos competitivos.

4.2.2 Impacto en Personas.

El impacto directo en el factor personas de los ve directamente reflejado en generar una cultura de prevención de riesgos así como también crear un ambiente en el cual se reporten todos los eventos suscitados en la

institución. Al mejorar el desarrollo personal cada uno de los funcionarios podrá evitar cometer errores e inclusive para quienes los errores forman parte de su remuneración variable les permitirán acceder a un mejor pago mensual

**CUADRO No 35.
MATRIZ DE IMPACTO EN PERSONAS**

INDICADOR	NIVEL DE IMPACTO						
	-3	-2	-1	0	1	2	3
Cultura de prevención					1		
Ambiente de entendimiento de riesgos					1		
reportes de errores						2	
incremento en cobro mensual						2	
TOTAL					2	4	0

Fuente: Propia

Elaboración: Autor del proyecto

$$\text{Nivel de impacto} = \frac{2 + 4 + 0}{4} = 1,50$$

En nivel de impacto en personas es positivo buscando incrementar una cultura de prevención de riesgos operativos y de aumento de reportes haciendo conciencia sobre la necesidad que tiene la institución de recopilar información de los factores de riesgo para evitar que se incurra en pérdidas por la exposición generada

4.2.3 Impacto en tecnología de Información.

El beneficio de todo el personal de Mutualista Imbabura es principalmente al acceder a cursos informáticos de calidad que aseguren un adecuado procedimiento de información y la continuidad del negocio en caso de fallas de los sistemas de TI.

CUADRO No 36
MATRIZ DE IMPACTO EN TECNOLOGÍA DE INFORMACIÓN

INDICADOR	NIVEL DE IMPACTO						
	-3	-2	-1	0	1	2	3
Sistema Informático parametrizado adecuadamente						2	
Adecuado procesamiento de información						2	
Continuidad de negocio						2	
TOTAL					0	6	0

Fuente: Propia

Elaboración: Autor del proyecto

$$\text{Nivel de impacto} = \frac{0 + 6 + 0}{4} = 1,50$$

El nivel de impacto en tecnología es positivo, el proyecto servirá para asegurar un adecuado manejo de información y la continuidad de las operaciones de la Mutualista Imbabura.

El impacto de factores externos es subjetivo y no podría ser descrito completamente por el gran número de posibles eventos a suscitarse por tal razón se mantiene un análisis de los principales factores de riesgo operativo.

3.5 MATRIZ GENERAL DE IMPACTOS.

CUADRO No 37
MATRIZ DE GENERAL

INDICADOR	NIVEL DE IMPACTO						
	-3	-2	-1	0	1	2	3
Impacto Social						2	
Impacto Económico					1		
Impacto Educativo					1		
TOTAL					2	2	0

Fuente: Propia

Elaboración: Autor del proyecto

$$\text{Nivel de impacto} = \frac{2 + 2 + 0}{4} = 1,33$$

En términos generales diríamos que el proyecto genera un nivel bajo positivo de acuerdo a la matriz de valoración, lo cual es bueno ya que se puede determinar que la implementación del Manual de Riesgo Operativo para Mutualista Imbabura es factible en todos los aspectos.

CONCLUSIONES Y RECOMENDACIONES

1. CONCLUSIONES.

Una vez que se ha diseñado el proyecto para la implementación del Manual de Riesgo Operativo en Mutualista Imbabura se puede afirmar que se ha llegado a alcanzar todos los objetivos propuestos. A continuación se enlistan las conclusiones del proyecto.

- a. No se cuenta con una base de eventos de riesgo operativo para determinar la adecuada severidad y frecuencia de los mismos.
- b. Se evidencia un alto nivel de temor del personal de la institución a reportar eventos de riesgo operativo por temor a los llamados de atención, multas o sanciones.
- c. Se detecta que existe una sola persona administrando todos los riesgos de la institución lo cual podría derivar en sanciones o multas por incumplimiento por parte del organismo de control
- d. El bajo nivel de conocimiento sobre el tema dentro del personal de mutualista Imbabura fue una limitante atada a la falta de información de consulta ya que el grado de aporte fue mínimo.
- e. Cuenta con herramientas informáticas adecuadas para el manejo de información y a su vez para el procesamiento de datos que permitan extraer la pérdida esperada de riesgo operativo.
- f. El presente trabajo de tesis delimita las funciones y responsabilidades de los funcionarios y áreas de la institución dentro de la administración de riesgo operativo, todo ello en base a la normativa vigente de riesgo operativo.

g. La propuesta define políticas generales y políticas específicas para la administración de riesgo operativo mejorando así el control de los factores como son procesos, personas, tecnología de información y eventos externos.

h. Se propone la utilización de procesos y procedimientos para la administración de riesgo operativo lo cual permite al personal ajeno al área de riesgos poder visualizar de mejor manera los pasos que se deberán seguir para poder desarrollar una adecuada implementación y control de riesgo operativo

i. El nivel de impactos analizado es positivo, lo que determina que el proyecto a ejecutarse es viable, en Mutualista Imbabura en beneficio tanto interno como externo.

2. RECOMENDACIONES.

a. Se recomienda la implementación del Manual de Riesgo Operativo ya que sería una guía adecuada para la administración de riesgo operativo en Mutualista Imbabura, puesto que actualmente no se cuenta con un documento que delimite funciones, políticas y procedimientos de tal forma que aseguren una adecuada gestión de riesgos así como también un adecuado ambiente de control interno dentro de todas y cada una de las áreas involucradas.

b. Se deberá capacitar al personal de la institución en temas relacionados a riesgo operativo para que posteriormente mediante su aporte se pueda mejorar el contenido del presente manual, considerando cambios normativos y requerimientos internos de la institución.

c. Se deberá mantener los niveles positivos de impactos y en caso de en la implementación del proyecto pudieran existir variaciones, tratar de enmendar los errores y solucionar los inconvenientes.

d. Se recomienda la dotación del recurso humano necesario para que la implementación del presente manual y la aplicación de su contenido tenga el éxito esperado.

GLOSARIO DE TÉRMINOS UTILIZADO EN EL MANUAL

- **A.M.A:** (Advanced Measurement Approach) Método de medición avanzada.
- **B.I.A:** (Basic Indicator Approach) Método del indicador básico
- **L.D.A:** (Loss Distribution Approach). Método de cálculo de pérdida operativa.
- **S.A.:** (Standard Approach) Método Estándar
- **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.
- **Evento de riesgo operativo:** Es el hecho que puede derivar en pérdidas financieras para la institución controlada.
- **Proceso:** Es el conjunto de actividades que transforman insumos en productos o servicios con valor para el cliente, sea interno o externo.
- **Insumo:** Es el conjunto de materiales, datos o información que sirven como entrada a un proceso.
- **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.

- **Actividad:** Es el conjunto de tareas.
- **Tarea:** Es el conjunto de pasos o procedimientos que conducen a un resultado final visible y medible.
- **Procedimiento:** Es el método que especifica los pasos a seguir para cumplir un propósito determinado.
- **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.
- **Datos:** Es cualquier forma de registro electrónico, óptico, magnético, impreso o en otros medios, susceptible de ser capturado, almacenado, procesado y distribuido.
- **Información:** Es cualquier forma de registro electrónico, óptico, magnético o en otros medios, previamente procesado a partir de datos, que puede ser almacenado, distribuido y sirve para análisis, estudios y toma de decisiones.
- **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.

- **Tecnología de información:** Es el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, servicios asociados, entre otros.
- **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.
- **Instalaciones:** Es la infraestructura que permite alojar los recursos físicos relacionados con la tecnología de información.
- **Responsable de la información:** Es la persona encargada de identificar y definir claramente los diversos recursos y procesos de seguridad lógica relacionados con las aplicaciones.
- **Seguridad de la información:** Son los mecanismos implantados que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella.
- **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.
- **Confidencialidad:** Es la garantía de que sólo el personal autorizado accede a la información preestablecida
- **Integridad:** Es la garantía de mantener la totalidad y exactitud de la información y de los métodos de procesamiento.

- **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.
- **Cumplimiento:** Se refiere a la observancia de las leyes, regulaciones y acuerdos contractuales a los que los procesos de las instituciones controladas están sujetos.
- **Plan de contingencia:** Es el conjunto de procedimientos alternativos a la operatividad normal de la entidad cuya finalidad es la de permitir su funcionamiento, buscando minimizar el impacto financiero que pueda ocasionar cualquier evento inesperado específico. El plan de contingencia se ejecuta el momento en que se produce dicho evento.
- **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.

Términos que concuerdan con los especificados en la resolución de la Junta Bancaria N° JB-2005-834 del 20 de octubre del 2005 emitida por la Superintendencia de Bancos y Seguros del Ecuador.

BIBLIOGRAFÍA.

Resolución JB-2005-834 de 20 de Octubre del 2005 de la Junta Bancaria sobre implementación de riesgo operativo en las instituciones Financieras.

Nuevo Acuerdo de Capitales (BASILEA II) prácticas internacionales. Riesgo operativo.

La Ley General de Instituciones del Sistema Financiero Vigente
2013-04-24

Diccionario Océano Uno Edición 2.008, Pag. 1.112

REYES P. Riesgo financieros Pag. 32, edición 2012.

Norma ASNZ ISO 31000 publicada en el mes de noviembre del
2009

Resolución No. JB-2004-631 del 22 de enero del 2004 de la
superintendencia de Bancos y Seguros del Ecuador

DAQUI R. define el riesgo de crédito Pag. 74, edición 2.006.

LIBRO I DE LAS NORMAS GENERALES PARA LA APLICACIÓN
DE LA LEY DE INSTITUCIONES DEL SISTEMA FINANCIERO,
mediante resolución JB-2002-429 del 22 de enero del 2002 y
reformado mediante resolución No. JB-2003-615 del 23 de
diciembre del 2003.

Codificación de resoluciones de la Superintendencia de Bancos y Seguros del Ecuador. Pag 204

Resolución No. JB-2008-1202 del 23 de octubre del 2008 de la Superintendencia de Bancos y Seguros del Ecuador.

Resolución No. JB-2005-834 de 20 de Octubre del 2005 de la Superintendencia de Bancos y Seguros,

Otero P. y Benerio O en su documento Metodología "Value at Risk" se refieren al método de medición avanzado AMA de riesgo operativo pag 69 edición 2008

Norma ISO/IEC 27001 de medición riesgos noviembre 2008

LINCOGRAFÍA.

[http://es.wikipedia.org/wiki/Mutualismo_\(biolog%C3%ADa\)](http://es.wikipedia.org/wiki/Mutualismo_(biolog%C3%ADa))

[http://lema.rae.es/drae/.](http://lema.rae.es/drae/)

[http://www.clubgestionriesgos.org/es/secciones/riesgo_operacional/introduccion/\)](http://www.clubgestionriesgos.org/es/secciones/riesgo_operacional/introduccion/)

<http://www.riesgooperacional.com/docs/22%20%20gacetabasilea-II-no6-riesgo-operacional.pdf>

http://es.wikipedia.org/wiki/Riesgo_operativo

Club de Gestión de Riesgos de España

<http://moodlexa.unsa.edu.ar/course/info.php?id=53>

<http://www.bridgedworld.com/es/soluciones/planes-de-contingencia>

http://www.abc.gob.bo/IMG/pdf/Cap_8-_SBX_Plan_de_contingencias.pdf

<http://definicion.de/diagnostico/>

http://www.corporacionsybven.com/portal/index.php?option=com_content&view=article&id=238: analisis-de-impacto&catid=124: conceptos-teoricos.

<http://es.thefreedictionary.com/teor%C3%ADa>

ANEXOS

ENTREVISTA CON LA GERENCIA GENERAL DE MUTUALISTA IMBABURA.

La presente entrevista tiene como finalidad recopilar información de mucha utilidad para el desarrollo del trabajo de investigación relacionado con la implementación de Un Manual de Riesgo operativo. Se requiere de la manera más comedida se dé respuesta a las siguientes preguntas:

¿Cuál ha sido el aporte de la administración en la implementación de riesgo operativo dentro de la institución?

¿Existe la apertura por parte de la administración para la capacitación del personal de la unidad de Riesgos en temas relacionados a riesgo operativo?

¿Considera usted necesario la dotación de personal para fortalecer la Unidad de Riesgos de la Institución?

¿La gerencia General o el Directorio realizan algún tipo de seguimiento a la implementación de Riesgo Operativo realizado principalmente por el Oficial de Riesgos?

¿Cómo considera la implementación de Riesgo operativo dentro de la Institución?

ENTREVISTA CON EL JEFE DE RECURSOS HUMANOS DE MUTUALISTA IMBABURA.

La presente entrevista tiene como finalidad recopilar información de mucha utilidad para el desarrollo del trabajo de investigación relacionado con la implementación de un manual de riesgo operativo. Se requiere de la manera más comedida se dé respuesta a las siguientes preguntas:

Primera parte: Estructura Administrativa.

¿La Estructura Orgánica de la institución contempla una Unidad de Riesgos debidamente constituida?

¿Se ha definido formalmente las funciones asignadas al personal de la Unidad de Riesgos en cuanto a sus obligaciones y responsabilidades?

¿El personal que labora en la Unidad de Riesgos de la institución cumple con los perfiles mínimos requeridos por la instrucción en cuanto a sus actitudes y aptitudes?

Segunda parte: Procesos levantados.

¿La institución cuenta con un mapa de procesos en los que los que se haya agrupado de acuerdo al requerimiento de la SBS (Gobernantes, Productivos y Habilitantes)?

¿Se han levantado los procesos identificados en la entidad?

Tercera Parte: Administración de Talento Humano.

¿La institución cuenta con un manual de administración del Recursos Humano?

¿En este manual se estipulan las políticas de Vinculación, permanencia y desvinculación del personal?

¿Se encuentran definidas las políticas de capacitación permanente al personal?

ENTREVISTA CON LA AUDITORA INTERNA DE MUTUALISTA IMBABURA.

La presente entrevista tiene como finalidad recopilar información de mucha utilidad para el desarrollo del trabajo de investigación relacionado con la implementación de Un Manual de Riesgo operativo. Se requiere de la manera más comedida se dé respuesta a las siguientes preguntas:

¿Dentro del Plan Anual de Evaluaciones de su área se contempla revisiones relacionadas al cumplimiento de riesgo operativo?

¿Con que frecuencia se realizan las supervisiones a la Unidad de Riesgos?

¿Cuáles son los temas dentro de riesgo operativo que se revisan en las supervisiones realizadas?

¿Qué criterio mantiene sobre el cumplimiento de la implementación de riesgo operativo a nivel general?

¿Qué criterio mantiene sobre el nivel de conocimiento sobre riesgo operativo del personal de la Unidad de Riesgo de la Institución?

¿Considera apropiado el aporte de recursos de la Alta Gerencia en la implementación de riesgo operativo?

¿Según su criterio considera apropiado el grado de exposición de riesgo operativo en la institución?

ENTREVISTA CON EL JEFE DE SISTEMAS DE MUTUALISTA IMBABURA.

La presente entrevista tiene como finalidad recopilar información de mucha utilidad para el desarrollo del trabajo de investigación relacionado con la implementación de un manual de riesgo operativo. Se requiere de la manera más comedida se dé respuesta a las siguientes preguntas:

¿En el área de sistemas se ha desarrollado un plan de contingencia que asegure la continuidad del uso del software informático?

¿Se cuenta con un manual de tecnología de información en donde se contemplen políticas relacionadas a riesgo operativo?

¿Cuenta con herramientas informáticas para la administración de riesgo operativo?

¿El sistema informático con el que opera la institución contiene un módulo de seguridad que permita controlar los accesos y la asignación de usuarios con sus respectivos roles?

¿El cumplimiento normativo de los requerimientos de TI dispuestos por la Superintendencia de bancos es adecuado?

ENCUESTA ANÓNIMA DIRIGIDA AL PERSONAL OPERATIVO Y DE SOPORTE DE LA MUTUALISTA IMBABURA.

La presente encuesta es anónima y tiene como finalidad recopilar información de mucha utilidad para el desarrollo del trabajo de investigación relacionado con la implementación de Un Manual de Riesgo operativo. Se requiere de la manera más comedida se dé respuesta a las siguientes preguntas de la manera más sincera posible:

- 1 ¿Ha asistido a cursos, charlas o talleres relacionados a riesgo operativo en el transcurso de su vida profesional?

SI _____ NO _____

3. ¿En esta institución ha recibido algún curso relacionado con riesgo operativo?

SI _____ NO _____

4. ¿Conoce usted cuales se denominan como factores de riesgo operativo?

SI _____ NO _____

5. ¿Ha utilizado el formato de reportes de eventos de riesgo operativo implantado por la Unidad de Riesgos de la Institución?

SI _____ NO _____

6. ¿Cuáles son las causas por las que Usted se debería limitado a no reportar los errores cometidos dentro de su puesto de trabajo?

- Temor a llamados de atención _____
- Temor a sanciones económicas _____
- Temor a perder el trabajo _____
- Otros _____
- Yo he reportado todo lo detectado _____

Explique _____ cuáles.

7. ¿Cuáles son sus principales fallas al momento de realizar las actividades para las que fue contratado en la institución?

- Errores de digitación de valores _____
- Errores de validación de estructuras _____
- Mal envío de documentos a impresoras _____
- Descuadres de caja (FALTANTE/SOBRANTE) _____
- Perdida de información causada por sistema _____
- Otros _____

Explique _____ cuáles.

8. Emita su criterio sobre la implementación de Riesgo operativo en la Institución.

Adecuado _____ Inadecuado _____

9. ¿Considera necesaria la implementación de un manual de riesgos en la institución?

SI _____ NO_____