

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS ECONÓMICAS Y FINANCIERAS
CARRERA DE CONTADURIA PÚBLICA



**MANUAL DE RIESGO OPERATIVO PARA ENTIDADES DEL
SECTOR PUBLICO FINANCIERO**

CASO: ENTIDADES FINANCIERAS NO BANCARIAS

**PROYECTO DE GRADO PRESENTADO PARA LA OBTENCION DEL GRADO DE
LICENCIATURA**

POR : ORLANDO GERMAN VINO CARRILLO

TUTOR : LIC. JUAN PEREZ VARGAS

LA PAZ - BOLIVIA
Septiembre, 2013

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS ECONÓMICAS Y FINANCIERAS
CARRERA DE CONTADURIA PÚBLICA

Proyecto de grado:

**MANUAL DE RIESGO OPERATIVO PARA ENTIDADES DEL
SECTOR PUBLICO FINANCIERO**

CASO: ENTIDADES FINANCIERAS NO BANCARIAS

Presentada por : Univ. Orlando German Vino Carrillo

Para optar el grado acaémico de *Licenciado en Contaduría Pública*

Nota numeral:

Nota literal:

Ha sido

Director de la carrera de Contaduría Pública: Lic. Gonzalo Terán Gandarillas

Tutor: Lic. Juan Pérez Vargas

Tribunal: Mg. Sc. Ausberto Choque Mita

Tribunal: Mgs Lic. Luis Alberto Mendoza M.

Tribunal: Mg. Sc. Ronny Yañez Mendoza

AGRADECIMIENTO

Al Supremo Creador DIOS, por darme la vida, la fuerza y sabiduría para mi formación académica e iluminar mi camino por la senda del éxito, y por no permitir que se anide en mi alma ningún sentimiento de resignación. A él le expreso mi infinito agradecimiento

A todos mis amigos y compañeros, por la compañía y los consejos a lo largo de toda mi formación académica y profesional, y me apoyaron en mis triunfos y vicisitudes, de quienes aprendí mucho.

DEDICATORIA

A mi madre, quien con su entusiasmo y ejemplo me inspiró para concluir con este proyecto.

A mi esposa, quien con cariño y paciencia me alentó para lograr concluir con este proyecto.

A mis hijos por la comprensión y paciencia por el tiempo utilizado en la dedicación a mi carrera profesional y para realizar este proyecto, y así demostrarles que nunca es tarde para lograr nuestros objetivos en la vida.

A todos aquellos amigos y personas que contribuyeron de alguna manera con sus consejos, ideas y correcciones en la realización de este trabajo.

**MANUAL DE RIESGO OPERATIVO PARA ENTIDADES DEL SECTOR PUBLICO
FINANCIERO NO BANCARIO**

CONTENIDO

CONTENIDO DE ILUSTRACIONES.....	i
ABREVIATURAS Y SIGLAS	ii
INTRODUCCION.....	1
CAPITULO I METODOLOGIA DE LA INVESTIGACION.....	4
1. PLANTEAMIENTO DEL PROBLEMA	4
2. FORMULACIÓN DEL PROBLEMA	5
3. JUSTIFICACION DEL PROYECTO.....	5
a) Justificación Teórica.....	5
b) Justificación Práctica	6
4. OBJETIVOS	7
a) Objetivo general del proyecto:.....	7
b) Objetivos Específicos:	7
5. METODOLOGIA DE LA INVESTIGACION	8
a) Estudio Descriptivo	8
b) Estudio Exploratorio.....	9
c) Estudio Explicativo	9
6. TÉCNICAS DE INVESTIGACIÓN.....	10
CAPITULO II MARCO CONCEPTUAL, TEORICO Y LEGAL	12
1. MARCO CONCEPTUAL.....	12
2. COMITÉ DE SUPERVISIÓN BANCARIA DE BASILEA.....	12
a) Antecedentes sobre el Acuerdo de Capital de Basilea (Basilea I).....	13
b) El Nuevo Acuerdo de Capital de Basilea (Basilea II)	13
c) Definición del Riesgo Operativo	14
d) Principios de Basilea II para la administración del Riesgo Operativo	16
3. COSO Y LOS NUEVOS ENFOQUES DE LA EVALUACIÓN DE RIESGOS.....	18
a) COSO I.....	18
b) Componentes del COSO I	20
i. Ambiente de Control.....	20
ii. Evaluación de Riesgos	20
iii. Actividades de control	21
iv. Información y comunicación.....	21
v. Supervisión.....	21

MANUAL DE RIESGO OPERATIVO PARA ENTIDADES DEL SECTOR PUBLICO FINANCIERO NO BANCARIO

c) Marco de Control Interno Basado en Riesgos COSO ERM (COSO II).....	21
d) Definición de Gestión de Riesgos Corporativos COSO II ERM.....	23
e) Componentes del COSO II – ERM.....	23
i. Ambiente interno.....	24
ii. Establecimiento de objetivos.....	24
iii. Identificación de eventos.....	24
iv. Evaluación de riesgos.....	24
v. Respuesta a los riesgos.....	25
vi. Actividades de control.....	25
vii. Información y comunicación.....	25
viii. Supervisión.....	25
4. GUÍA PARA LAS NORMAS DEL CONTROL INTERNO DEL SECTOR PÚBLICO.....	26
a) Definición de Gestión de Riesgos de la Entidad INTOSAI.....	27
b) Gerencia de Riesgos de la Entidad - GRE.....	27
c) Componentes de la Gerencia de Riesgos de la Entidad.....	32
5. NORMA AS/NZS 4360: 2004 DE ADMINISTRACIÓN DE RIESGOS.....	34
a) Definiciones de la Administración de Riesgos de la AS/NZS 4360:2004.....	35
b) Elementos del proceso de Administración de Riesgos AS/NZS 4360: 2004.....	37
6. ISO 31000 GESTIÓN DE RIESGOS.....	43
a) Definiciones de la Gestión de Riesgos ISO 31000.....	44
b) Principios de la Gestión de Riesgos.....	45
c) Marco de Gestión del Riesgo.....	47
i. Mandato y el compromiso (4.2).....	48
ii. Diseño del marco para la gestión de riesgo (4.3).....	49
iii. Implementando la gestión de riesgos (4.4).....	53
iv. Seguimiento y revisión del marco (4.5).....	54
v. La mejora continua del marco (4.6).....	54
d) Proceso de Gestión del Riesgo.....	55
i. Comunicación y consulta.....	55
ii. Establecer el contexto: (5.3).....	56
iii. Evaluación del riesgo: (5.4).....	58
iv. Tratamiento del riesgo: (5.5).....	61
e) Aplicación y Beneficios de la Norma ISO 31000.....	63

**MANUAL DE RIESGO OPERATIVO PARA ENTIDADES DEL SECTOR PUBLICO
FINANCIERO NO BANCARIO**

7. MARCO TEÓRICO Y LEGAL.....	64
7.1 Principios, Normas Generales y Básicas de Control Gubernamental	65
7.2 Marco Legal del Sistema de Control Interno Gubernamental Boliviano	66
a) Conceptualización del control interno.....	67
b) Estructura de los Principios, Normas Generales y Básicas de Control Interno	68
7.3 Guía para la aplicación de los principios, normas Generales y Básicas de Control Interno Gubernamental CI/10	69
a) Estructura de la Guía CI/10	69
b) Evaluación de Riesgos según CI/10.....	70
c) Concepto de Riesgos según CI/10	71
7.4 Guía para la implantación del Control Interno G/CE-21	71
a) Objetivo y estructura de la Guía G/CE-21	71
b) Evaluación de Riesgos según la Guía G/CE-21.....	72
c) Subcomponentes de la Evaluación de Riesgos según la Guía G/CE-21.....	72
i. Subcomponente: Identificación de Eventos	73
ii. Subcomponente: Evaluación de Riesgos	79
iii. Subcomponente: Respuesta a los Riesgos.....	86
7.5 Mapa de Riesgos	92
CAPITULO III MANUAL DE RIESGO OPERATIVO	95
1. ANTECEDENTES.....	95
2. AMBITO DE APLICACION	96
3. ENTIDADES DEL SECTOR PÚBLICO FINANCIERO NO BANCARIO.....	98
4. CICLO OPERATIVO Y FINANCIERO DE LA ENTIDADES FINANCIERAS NO BANCARIAS	99
a) Captación	100
b) Colocación	100
c) Recuperación.....	101
d) Pagar el Servicio de la Deuda	101
e) Re inversión	101
5. ENFOQUE Y METODOLOGÍA PROPUESTA DE LA GESTIÓN DE RIESGO....	102
a) Cultura y Compromiso.....	103
b) Establecimiento del Marco de la Gestión de Riesgos.....	104
c) Proceso de la Gestión de Riesgos	104

**MANUAL DE RIESGO OPERATIVO PARA ENTIDADES DEL SECTOR PUBLICO
FINANCIERO NO BANCARIO**

6.	PROPUESTA DE MANUAL DE RIESGO OPERATIVO	105
6.1	Introducción	105
6.2	Principios de la Gestión de Riesgos.....	107
6.3	Políticas Institucionales de Administración del Riesgo	109
6.4	Estructura, Funciones y Responsabilidades	110
6.5	Responsabilidad del Directorio o Comités Ejecutivos.....	110
6.5.1	Comité de Riesgos.....	111
6.5.1.1	Obligaciones del Comité de Riesgos	112
6.5.1.2	Funciones.....	112
6.5.1.3	Modificación de Límites	113
6.5.1.4	Reuniones del Comité de Riesgos	113
6.5.1.5	Reglamento Interno de Trabajo del Comité de Riesgos	113
6.5.1.6	Requisitos de los Miembros del Comité de Riesgos	113
6.5.1.7	Periodo de Vigencia	114
6.5.2	UNIDAD DE RIESGOS	114
6.5.2.1	Funciones.....	114
6.5.2.2	Recursos Materiales de la Unidad de Riesgo	114
6.5.2.3	Comunicaciones de la Unidad de Riesgo con Auditoría Interna.....	115
6.5.3	JEFE O RESPONSABLE DE LA UNIDAD DE RIESGOS	115
6.5.3.1	Responsabilidad.....	115
6.5.3.2	Funciones.....	115
6.5.3.3	Requisitos del Responsable de la Unidad de Riesgos	116
6.5.3.4	Impedimentos.....	118
6.5.4	DE LA UNIDAD DE AUDITORÍA INTERNA	118
6.5.5	DE LAS UNIDADES DE LA ENTIDAD	118
6.6	MARCO LEGAL Y TECNICO	119
6.6.1	Normativa Nacional.....	119
6.6.2	Normas técnicas internacionales.....	120
6.7	MARCO CONCEPTUAL.....	120
6.7.1	Factores de Riesgo.....	122
6.7.2	Mapa de procesos	123
6.8	METODOLOGIA	124

MANUAL DE RIESGO OPERATIVO PARA ENTIDADES DEL SECTOR PUBLICO FINANCIERO NO BANCARIO

6.8.1 ESTABLECIMIENTO DEL CONTEXTO.....	126
6.8.2 IDENTIFICACIÓN DE RIESGOS.....	128
6.8.3 EVALUACIÓN DE RIESGOS (ANALISIS DE RIESGOS).....	133
6.8.3.1 Calificación del Riesgo.....	134
6.8.3.2 Evaluación del Riesgo.....	138
6.8.3.3 Determinación del nivel del riesgo (Valoración del Riesgo).....	139
6.8.4 POLÍTICAS DE ADMINISTRACION DE RIESGOS.....	143
6.8.4.1 Elaboración del Mapa de Riesgos por proceso y el institucional.....	145
6.8.4.2 Descripción del Mapa de riesgos.....	145
6.8.4.3 Priorización de los riesgos.....	146
6.8.5 MONITOREO Y CONSULTA.....	148
6.8.6 DOCUMENTACIÓN SOPORTE DE LA GESTIÓN DE RIESGOS.....	149
6.8.7 GLOSARIO Y DEFINICION DE TERMINOS.....	149
CAPITULO IV CONCLUSIONES Y RECOMENDACIONES.....	153
1. CONCLUSIONES.....	153
2. RECOMENDACIONES.....	154
BIBLIOGRAFIA.....	156

**MANUAL DE RIESGO OPERATIVO PARA ENTIDADES DEL SECTOR PUBLICO
FINANCIERO NO BANCARIO**

CONTENIDO DE ILUSTRACIONES

FIGURA 1 PILARES DE BASILEA II	14
FIGURA 2 MARCO DE COSO	20
FIGURA 3 RELACIÓN ENTRE COSO I Y COSO II.....	22
FIGURA 4 COMPONENTES COSO II - ERM.....	26
FIGURA 5 RIESGOS QUE ENFRENTAN LOS GOBIERNOS	31
FIGURA 6 PROCESO DE ADMINISTRACIÓN DE RIESGOS.....	39
FIGURA 7 ESQUEMA DE LA RELACIÓN ENTRE LOS PRINCIPIOS, ESTRUCTURA Y PROCESO.....	44
FIGURA 8 MARCO DE LA GESTIÓN DEL RIESGO	48
FIGURA 9 RELACIÓN ENTRE LOS PROCESOS	55
FIGURA 10 MATRIZ DE CONFIGURACIÓN DE EVENTOS.....	76
FIGURA 11 MATRIZ DE EVENTOS – HORIZONTAL Y VERTICAL.....	77
FIGURA 12 MATRIZ DE EVENTOS INTERRELACIONADOS.....	79
FIGURA 13 FRECUENCIA DE OCURRENCIAS (FO)	81
FIGURA 14 IMPORTANCIA RELATIVA (IR)	83
FIGURA 15 MATRIZ DE NIVEL DE RIESGOS.....	84
FIGURA 16 MATRIZ PARA LA VALORACIÓN DE EVENTOS CORRELACIONADOS	86
FIGURA 17 MATRIZ DE RESPUESTA AL RIESGO	89
FIGURA 18 ÁMBITO DEL SECTOR PÚBLICO.....	97
FIGURA 19 CICLO OPERATIVO Y FINANCIERO DE LAS ENTIDADES FINANCIERAS	99
FIGURA 20 MAPA DE PROCESOS CLAVES	124

MANUAL DE RIESGO OPERATIVO PARA ENTIDADES DEL SECTOR PUBLICO FINANCIERO NO BANCARIO

ABREVIATURAS Y SIGLAS

COSO:	Committe of Sponsoring Organizations
ERM-COSO:	Enterprise Risk Management (COSO II)
INTOSAI:	Organización Internacional de las Entidades Fiscalizadoras Superiores
AS/NZS:	Norma Australiana Neozelandesa de Gestión de Riesgo
ISO:	International Organization for Standardization
BIS:	Banco de Pagos Internacionales
AICPA:	Instituto Americano de Contadores Públicos Certificados
GRE:	Gerencia de Riesgos de la Entidad
SAFCO:	Sistemas De Administración Financiera y Control Gubernamental
FPS:	Fondo de Inversión Productivo y Social
FONDESIF:	Fondo de Desarrollo del Sistema Financiero y de Apoyo al Sector Productivo
FOFIM:	Fondo De Financiamiento para La Minería
FNDR:	Fondo Nacional de Desarrollo Regional
FONADAL:	Fondo Nacional de Desarrollo Alternativo
FDC:	Fondo de Desarrollo Campesino

INTRODUCCION

Riesgo es el daño potencial que puede surgir por un proceso presente o suceso futuro. Si, de acuerdo a esta definición podemos decir que el riesgo está latente en cualquier actividad o proceso que se realice sin que podamos determinar el momento de su ocurrencia pero si realizar o tomar medidas preventivas para minimizar la probabilidad de ocurrencia y el impacto que pueda tener. Las organizaciones sin importar su actividad o giro del negocio se enfrentan constantemente a diversos tipos de riesgos con los cuales deben convivir, sin que exista un mecanismo 100% confiable o seguro que permita evitar dichos riesgos.

Aunado a las grandes pérdidas sufridas por fallos operativos en las instituciones financieras privadas y públicas durante los últimos años, bajo un contexto de mayor sofisticación de operativa bancaria a nivel internacional, ha llevado a una mayor concientización de la importancia del riesgo operativo y a un interés por la mejora de los sistemas de control interno en las entidades financieras, conciencia de control basado en riesgos que podría ser aplicable al Sector Público Financiero no Bancario.

Todo ello ha motivado a los organismos reguladores a considerar explícitamente este riesgo entre sus criterios de vigilancia y supervisión. De esta manera, en enero de 2001 el Comité de Supervisión Bancaria de Basilea (Basilea II) incluyó, por primera vez, un requerimiento de capital por riesgo operativo en su propuesta para un “Nuevo Acuerdo de Capital”.

Este documento ha sido el detonante de un intenso proceso de colaboración entre el Comité, las instituciones financieras y otros organismos independientes, que ha llevado a la publicación de documentos donde se definen las mejores prácticas para una efectiva gestión y supervisión del riesgo operativo.

El objetivo final de este proyecto es el de demostrar la aplicabilidad de la gestión integral del riesgo operativo en entidades del Sector Público Financiero no Bancario del Estado Boliviano utilizando los conceptos del Comité de Basilea, el enfoque ERM-COSO (Marco de Control Interno Organizacional basado en el riesgo), Norma AS/NZS

4360:2004 Estándar Australiano de Administración de Riesgos, y la norma ISO 31000 de Gestión del Riesgo – Principios y Directrices. En el ámbito Boliviano se utilizó la base conceptual de los Principios, Normas Generales y Básicas de Control Interno Gubernamental así como la Guía para las normas de Control Interno del Sector Público de la INTOSAI (Organización Internacional de las Entidades Fiscalizadoras Superiores).

En la primera parte de este proyecto, se abordan el planteamiento del problema, la justificación del proyecto, los objetivos y el marco metodológico utilizado para realizar la investigación.

La segunda parte da énfasis al marco conceptual, teórico y legal donde se realiza una revisión de una breve reseña histórica, objetivos y funciones del Comité de Supervisión Bancaria de Basilea (Basilea II), evolución del control interno hasta llegar al modelo *COSO II (ERM-COSO Marco de Control Interno Organizacional basado en el riesgo)*, los modelos de gestión del Riesgo de la *norma Australiana NS/NZS 4360:2004 de Administración del riesgo* y la *norma ISO 31000 de Gestión del Riesgo – Principios y Directrices*, así como la *Guía para las Normas del Control Interno del Sector Público* de la INTOSAI en su documento “*Información adicional sobre la Administración de Riesgos de la Entidad*” (INTOSAI GOV 9130) y los *Principios, Normas Generales y Básicas de Control Interno Gubernamental* de Sector Público Boliviano.

En la tercera parte se desarrolla proyecto, comenzaremos a describir las mejores prácticas para la Gestión del Riesgo Operativo, tomando como base los principios fundamentales, conceptos, marco teórico y procedimientos aplicables al Sector Público Boliviano de los modelos de gestión de riesgo descritos y analizados en la Parte II, seguidamente, en esta misma parte nos referimos al Riesgo Operativo, detallando cada una de las implicaciones que tiene este tipo de riesgo en el Sector Público Financiero no Bancario.

Se plantea que las instituciones financieras del sector público deben desarrollar un sistema de gestión integral de riesgos operativos que garanticen la efectiva gestión, evaluación y control del riesgo operativo, y para crearlos, usaremos los lineamientos de

los diferentes modelos de gestión y evaluación del Riesgo, quienes han impulsado una serie de herramientas de gestión, como mapas de riesgo, auto evaluaciones, base de datos internas y externas, etc.

Describiremos un marco de gestión donde se vea identificado los principales objetivos que deben alcanzar o poner en práctica las instituciones públicas del Sector Público Financiero no Bancario, de esta manera definiremos las mejores práctica para la gestión y vigilancia de riesgo operativo; y un modelo conceptual y metodológico de gestión de riesgos operativos que se traducirá en un modelo de Manual de Riesgo Operativo.

La parte final del proyecto estable las conclusiones y recomendaciones sobre la aplicabilidad de la gestión integral del Riesgo Operativo en entidades del Sector Público Financiero no Bancario, utilizando como referente la escasa normativa técnica y legal emitida por la Contraloría General del Estado y otras entidades que emiten normas respecto a este tema, reforzada por la normativa técnica y conceptual de la ISO 31000, *Norma Australiana NS/NZS 4360:2004* y *Guía INTOSAI*.

Con el objetivo final de que sea una propuesta de política de Gestión y Control Gubernamental la implantación de la gestión del Riesgo Operativo en el Sector Público Financiero no Bancario de Bolivia y en general para todo el sector Público Boliviano.

CAPITULO I METODOLOGIA DE LA INVESTIGACION

1. PLANTEAMIENTO DEL PROBLEMA

A raíz que el Comité de Supervisión Bancaria de Basilea, del Banco de Pagos Internacionales (BIS), ha incluido la Gestión de Riesgo Operativo como parte de las mejores prácticas de Gestión de Riesgos en las entidades financieras, los supervisores bancarios de muchos países, han iniciado el camino para adaptar a las regulaciones locales siguiendo los requerimientos del documento consultivo del Nuevo Acuerdo de Capital de Basilea (Basilea II).

Debido a la innovación de la gestión del riesgo operativo, es que se pretende aplicar al Sector Público Financiero no Bancario que si bien tienen competencias y objetivos definidos por ley, estas entidades no están exentas del riesgo operacional que puede generar pérdidas no cuantificables u ocultas o el incumplimiento en logro de objetivos institucionales y a su vez generar responsabilidad por la función pública.

Se plantea los siguientes problemas:

- No existe norma legal o técnica que defina los alcances y la implementación de la Gestión Integral del Riesgo Operativo en el Sector Público Financiero no Bancario y en el Sector Público Boliviano en general.
- No existen bibliografías específicas, donde se realice el análisis teórico y conceptual de los requisitos incluidos Basilea II, del modelo ERM-COSO y otros modelos de Gestión de Riesgos aplicables al Sector Público Financiero no Bancario.
- No existen métodos o modelos de gestión definidos, que ayuden a las instituciones públicas financieras no bancarias, a implantar un modelo para la gestión del riesgo operativo y la administración de riesgos en general.

2. FORMULACIÓN DEL PROBLEMA

Las entidades del Sector Público Financiero no Bancario no poseen las herramientas básicas que les permitan realizar una gestión de sus riesgos operativos así como la administración de los mismos, es decir, no realizan la administración de riesgos y aún no existe una metodología de evaluación y gestión integral de los riesgos operativos, mediante la aplicación instrumentos normativos, metodológicos, teóricos y de buenas prácticas para la administración del riesgo operacional en este tipo de entidades.

Debido a que es importante la gestión pública en el actual contexto político económico y social que atraviesa el país, definido en una nueva Constitución Política del Estado, donde ya se definen actores como el control social que velaran por una adecuada gestión pública y para cumplir con sus objetivos las entidades deben tener en cuenta la gestión integral del riesgo operativo con el objeto de establecer una “cultura de control de riesgos operativos”.

3. JUSTIFICACION DEL PROYECTO

Conforme fue evolucionando la evaluación del control interno a una enfoque basado en riesgos aunado a los estándares emitidos por el Comité de Supervisión Bancaria de Basilea (Basilea II), donde vieron la importancia de la gestión integral del riesgo operativo en entidades financieras, en particular, al tener como mercancía objeto de su negocio el “dinero”, es por ello que las entidades del Sector Público Financiero no Bancario, que realizan actividades crediticias para el desarrollo económico - social de determinados sectores públicos y privados, se encuentran inmersos dentro del denominado “concepto global de riesgo”, por lo que su gestión debe convertirse en pieza clave no solo de su éxito sino de su supervivencia.

a) Justificación Teórica

La investigación propuesta busca por medio del conocimiento de la teoría de la gestión del riesgo, los lineamientos emitidos por el Comité de Supervisión Bancaria

CAPITULO I Metodología de la Investigación

de Basilea (Basilea II), el modelo ERM-COSO (Marco de Control Interno Organizacional basado en el riesgo) y otros modelos de gestión de riesgos como la Norma ISO 31000 “Gestión del Riesgo”; la Norma NS/NZS 4360:2004 Estándar Australiano de Administración de Riesgos; Guía para las Normas de Control Interno del Sector Público – Información adicional sobre la Administración de Riesgos de la Entidad (INTOSAI GOV 9130) de la INTOSAI y los Principios, Normas Generales y Básicas de Control Interno Gubernamental del Sector Público Boliviano; estructurar una metodología de gestión integral del riesgo operativo en un sentido amplio, es decir, su identificación, evaluación, seguimiento o supervisión y control y debe proyectarse a todos los niveles organizativos de las entidades del Sector Público Financiero no Bancario.

La investigación de la teoría acerca de los modelos de la administración de riesgo operativo y la gestión integral del mismo permitirá encuadrar los mismos en el contexto actual y real capaz de ser aplicable al Sector Público Financiero no Bancario.

Por lo tanto el tema de investigación pretende diseñar un sistema de gestión integral del Riesgo Operativo eficiente que ayude a prevenir de posibles riesgos que podrían ocasionar pérdidas y/o el incumplimiento de objetivos institucionales e inclusive generar responsabilidades por la función pública en las Entidades del Sector Público Financiero no Bancario.

b) Justificación Práctica

El proyecto busca determinar la utilidad del sistema de gestión integral de Riesgo Operativo aplicable a las Entidades del Sector Público Financiero no Bancario, con el cual se pretende dar respuesta a la problemática de la gestión del riesgo en el Sector Público en General.

Es un tema poco estudiado mucho menos aplicado al Sector Público Financiero no Bancario, por esto la importancia, para determinar los fundamentos teóricos,

metodológicos y técnicos que nos van a permitir realizar una aplicación práctica de la administración del riesgo operativo y su gestión integral.

Debido a que el mero control “a posteriori” resulta ya insuficiente e ineficiente y junto a una clara concienciación sobre su importancia, es viable crear un entorno de control preventivo basado en riesgos que favorezca su gestión de manera eficaz y eficiente.

La gestión de este riesgo tiene su justificación en la pérdida potencial o incumplimiento de objetivos derivada de deficiencias significativas en la integridad o confianza de las operaciones (Producción ó Servicio) de las entidades públicas general y en especial de las entidades del Sector Público Financiero no Bancario.

4. OBJETIVOS

a) Objetivo general del proyecto:

Establecer una metodología para la identificación, medición, evaluación, administración y gestión del Riesgo Operativo utilizando las herramientas para la gestión del Riesgo Operativo del Nuevo Acuerdo de Capital de Basilea (Basilea II) e instrumentos del modelo ERM-COSO (Marco de Control Interno Organizacional basado en el riesgo) y los otros modelos de Gestión de Riesgos aplicables para las entidades del Sector Público Financiero no Bancario el cual será traducido en un Manual de Riesgo Operativo.

b) Objetivos Específicos:

- Introducción del marco teórico y conceptual que sirva de apoyo a las entidades del Sector Público Financiero no Bancario, que deben implantar modelos de gestión de riesgo operativo utilizando los parámetros establecidos por el Comité de Supervisión Bancaria de Basilea (Basilea II) aplicables al Sector Público y el modelo ERM-COSO conforme a la “Guía para la aplicación de los principios,

normas generales y básicas de control interno gubernamental” así como los otros modelos de gestión de riesgos.

- Abordar de manera descriptiva las implicaciones (fortalezas y retos) que tiene la gestión del Riesgo Operativo en las Entidades del Sector Público Financiero no Bancario.
- Analizar las diferentes herramientas metodológicas y criterios que deben cumplir las Entidades del Sector Público Financiero no Bancario para determinar una metodología de identificación, medición, monitoreo y administración del Riesgo Operativo.
- Analizar la evolución y aplicación de las normas y lineamientos sobre la gestión del Riesgo Operativo por parte de las Entidades del Sector Público Financiero no Bancario.
- Analizar la forma en que las herramientas informáticas apoyan en la gestión del Riesgo Operativo.
- Determinar la forma en que el control interno interviene dentro de la cadena de valor de una Entidad del Sector Público Financiero no Bancario y el impacto que ésta genera.

5. METODOLOGIA DE LA INVESTIGACION

El tipo de investigación utilizado para recopilar la información necesaria es exploratoria, descriptiva y explicativa; la cual permite determinar los orígenes o causas del planteamiento del problema, y explicar las implicaciones del mismo.

a) Estudio Descriptivo

Los estudios descriptivos buscan especificar las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que sea sometido a análisis. Desde el punto de vista científico, describir es medir

El estudio descriptivo acude a técnicas específicas en la recolección de información, y para ello utilizaremos el análisis documental y entrevistas para describir los modelos existentes, si estos hubieren.

Por lo tanto identificamos el marco conceptual, teórico, regulatorio internacional y cualquier modelo aplicado en el sector financiero privado, como es el de Basilea II y el modelo ERM-COSO y otros modelos de gestión de riesgo como la ISO 31000, el Estándar Australiano AS/NZS 4360:2004 y la Guía INTOSAI GOV 9130, que se pretende introducirlo en el ámbito del sector público específicamente al financiero no bancario.

b) Estudio Exploratorio

La investigación es exploratoria cuando no utilizas ningún modelo anterior como base de un estudio. Podríamos normalmente tomar una teoría anterior como una ayuda, pero quizás no hay ninguna, o todos los modelos disponibles vienen de contextos impropios o diferentes.

La investigación exploratoria significa que muy poco se sabe sobre la materia o tema de estudio del proyecto.

Por lo tanto, nuestro estudio es exploratorio porque no existe un marco teórico, legal y técnico específico referido a la gestión del Riesgo Operativo en Entidades del sector Público Boliviano e inclusive a nivel mundial.

c) Estudio Explicativo

Los estudios explicativos van más allá de la descripción de conceptos o fenómenos, están dirigidos a responder a las causas de los eventos físicos o sociales. En este proyecto enfocaremos como estudio explicativo para responder las causas de los modelos de gestión de riesgo del sector privado existentes a nivel mundial.

Esto nos permitirá la explicación de la forma, metodología y proceso de implementación de la gestión de Riesgo Operativo en el Sector Público Financiero no Bancario del Estado Plurinacional de Bolivia.

6. TÉCNICAS DE INVESTIGACIÓN

Debido a que el tema propuesto es inédito en el ámbito nacional, debido a que aun no existe un marco legal, teórico y técnico definido sobre la gestión del Riesgo Operativo aplicable al sector público o privado, es que se utilizó la Investigación Documental, porque esta se constituye en una variante de la investigación científica, cuyo objetivo fundamental es el análisis de diferentes fenómenos (de orden históricos, psicológicos, sociológicos, etc.), utiliza técnicas muy precisas, de la documentación o material existente, que directa o indirectamente, aporte información para el proyecto.

Se utilizó la investigación documental como parte del proceso de investigación científica, como una estrategia porque con esta observamos y reflexionamos sistemáticamente sobre realidades (teóricas o no) usando para ello diferentes tipos de documentos de otros países, obtenidos básicamente mediante el internet.

Se indago e interpreto los datos, información, y documentos existentes sobre la gestión del Riesgo Operativo en el Sector Financiero Privado a nivel mundial, para luego proponer su aplicabilidad en el Sector Público Financiero no bancario Boliviano.

La investigación documental se caracteriza por:

- La utilización de documentos y material recolectado, seleccionado y analizado para presentar resultados coherentes.
- Utiliza los procedimientos lógicos y mentales de toda investigación; análisis, síntesis, deducción, inducción, etc.
- Realiza una recopilación adecuada de datos que permiten redescubrir hechos, sugerir problemas, orientar hacia otras fuentes de investigación, orientar formas para elaborar instrumentos de investigación, elaborar hipótesis, etc.

CAPITULO I Metodología de la Investigación

- Es una investigación que se realiza en forma ordenada y con objetivos precisos, con la finalidad de ser base para la construcción de conocimientos, es decir, en la proposición de nuevos proyectos como el que se plantea en este documento.
- Se ha utilizado diferentes técnicas de: localización y fijación de datos, análisis de documentos y de contenidos, por ejemplo mediante internet se obtuvo información de los Bancos Centrales del Mundo que inician procesos de implantación de la Gestión del Riesgo Operativo, el sector financiero Mundial que también realiza esfuerzos en la implantación de esta gestión.

En un sentido restringido, entendemos a la investigación documental como un proceso de búsqueda que se realiza en fuentes impresas (documentos escritos), como también fuentes electrónicas (páginas web's, libros electrónicos, papers y publicaciones en PDF), es decir, se realiza una investigación bibliográfica especializada para producir nuevos asientos bibliográficos sobre el particular.

Sin embargo no se puede confundir como iguales, a la investigación bibliográfica y a la investigación documental. Esta afirmación como podemos observar, reduce la investigación documental a la revisión y análisis de libros dejando muy pobremente reducido su radio de acción.

La investigación bibliográfica, es un cuerpo de investigación documental. Asumimos la bibliografía como un tipo específico de documento, pero no como el Documento.

CAPITULO II MARCO CONCEPTUAL, TEORICO Y LEGAL

1. MARCO CONCEPTUAL

Con el fin de proponer una alternativa sobre la administración del riesgo operativo aplicable al Sector Público Financiero no Bancario se pretende desarrollar un modelo de gestión de riesgo operativo, sobre la base conceptual del marco regulatorio de Basilea II, el modelo de control interno COSO II (ERM-COSO Marco de Control Interno Organizacional basado en el riesgo) el Estándar Australiano de Administración de Riesgos AS/NZS 4360:2004 y la norma ISO 31000 de Gestión del Riesgo – Principios y Directrices, adicionalmente se ha tomado en cuenta los Principios, Normas Generales y Básicas de Control Interno Gubernamental, y debido a que estos enfoques o modelos son de aplicación obligatoria en el caso de Basilea II y aplicación práctica del modelo COSO II en el sector privado financiero; es que se utilizaran las herramientas, metodologías, procedimientos, lineamientos, instrumentos y prácticas que pueden ser aplicables al sector público.

Para ello realizaremos una revisión de los siguientes antecedentes, documentos y marco conceptual:

2. COMITÉ DE SUPERVISIÓN BANCARIA DE BASILEA

Debido a que este comité se estudia el mercado y el negocio a nivel macro y a partir de allí, hacen recomendaciones de carácter general, frente a debilidades manifestadas de muchos sistemas bancarios que podrían amenazar la estabilidad financiera y comprometer la clara tendencia, ya entonces advertida, hacia la globalización.

Entre los documentos publicados se encuentra el actual Acuerdo de Capital de Basilea, siendo este aceptado y adoptado por más de 100 países en la actualidad.

a) Antecedentes sobre el Acuerdo de Capital de Basilea (Basilea I)

Después la implantación del Acuerdo de Capital de Basilea I, durante la evaluación constante de este documento, el comité recogió los comentarios y observaciones de la banca a nivel mundial, emitiendo formalmente, en 1999, el primer documento consultivo donde se planteaba los objetivos de la elaboración global de la suficiencia de capital, y en el mismo se sugiere requerimientos de adecuación de capital por el riesgo operativo.

b) El Nuevo Acuerdo de Capital de Basilea (Basilea II)

En el año 2001, el comité, emite un segundo documento consultivo, el cual incorpora de manera firme, requerimientos de adecuación de capital por el riesgo operativo, presentando la versión definitiva del **Nuevo Acuerdo de Capital de Basilea (Basilea II)**, en el año 2006.

El comité reconoce que Basilea II es más extenso y más complejo que Basilea I, esto no es más que el resultado de los esfuerzos del comité por elaborar un marco sensible al riesgo, que ofrece además una serie de nuevas opciones para medir tanto el riesgo crediticio como el operativo.

Los objetivos de Basilea II buscan poner más énfasis en la gestión del riesgo y fomentar mejoras continuas en la capacidad de los bancos para evaluarlos, buscando la adecuación de capital en las entidades financieras a los riesgos reales incurridos en la actividad bancaria, así como verificar que ese especial interés que se pone en el riesgo, trascienda en la eficacia de las prácticas de los supervisores y fortalezca la disciplina del mercado, mediante la generación de incentivos para mejorar las capacidades de medición y gestión del riesgo así como la divulgación de información, tanto sobre el mismo como sobre el capital.

Desde el 2007 hasta la actualidad, se encuentra vigente el Acuerdo de Basilea II que está estructurado en tres pilares fundamentales véase la Figura 1:

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

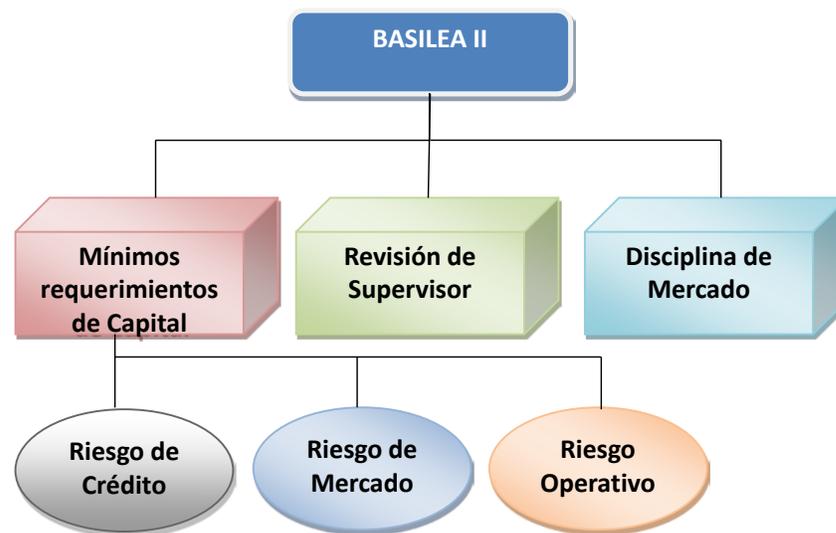


Figura 1 Pilares de Basilea II

c) Definición del Riesgo Operativo

En Nuevo Acuerdo de Basilea (Basilea II), recomienda como conveniente un tratamiento específico para el denominado Riesgo Operativo, entendido como aquel que se refiere a las **posibles pérdidas que pueden presentarse como resultado de procesos, personal o sistemas internos inadecuados o defectuosos, o hechos externos que afecten el banco**. Este reconocimiento explícito, refleja el interés del comité de Basilea, en hacer que el Nuevo Acuerdo de Capital sea más sensible al riesgo.

CAPITULO II Marco Conceptual, Teórico y Legal

Así también se realizará el análisis de las causas de la inclusión del riesgo operativo en Basilea II, y este surge de la preocupación del Comité, por considerarlo de gran importancia para los bancos, quienes deben mantener el capital necesario para protegerse de las posibles pérdidas que por ellos se ocasionen. Entre los principales factores están las siguientes:

1. La globalización ha aumentado la complejidad de productos y servicios ofrecidos por las instituciones bancarias a nivel internacional.
2. Crecimiento de los medios electrónicos, usados como base primordial de las operaciones de las instituciones financieras.
3. Gran número de fusiones y adquisiciones de empresas financieras, que se han llevado a cabo a gran escala a nivel mundial y que ponen a prueba la integración de sistemas y procesos.
4. Alto grado de automatización tecnológica presente en el sistema financiero mundial.
5. Mayor oferta y contratación de proveedores de servicios (Outsourcing).
6. Desarrollo de nuevos productos y servicios, que cada día son más complejos, lo que ha ocasionado una paulatina transformación de los bancos en grandes proveedores de servicios.
7. Crecimiento de volúmenes de negocio en el sistema.

El comité, con el propósito de aclarar la definición de riesgo operativo, realiza la clasificación de los tipos de eventos de pérdidas, para ello define ciertas características de los tipos de pérdidas (directas, indirectas, esperadas e inesperadas).

Pérdidas directas: Pérdidas como consecuencias “directas” de la materialización del evento de riesgo operativo, como por ejemplo el dinero que se pagaría en caso de la imposición de multas por los organismos reguladores.

Pérdidas indirectas: pérdidas para “solucionar” un problema de riesgo operacional, como por ejemplo, los gastos incurridos en la contratación de abogados que se encarguen de solucionar o defender a la institución ante una demanda.

Pérdidas esperadas (EL): Como lo muestra la figura 3, son eventos de pérdidas que generalmente son de bajo impacto monetario pero de alta frecuencia o probabilidad de ocurrencia.

Pérdidas inesperadas (UL): Eventos de pérdidas de alto impacto monetario y de baja frecuencia.

Adicionalmente el comité define siete tipos generales de categorías de pérdidas operacionales que pueden afectar a las instituciones financieras, a saber, a) Fraude Interno, b) Fraude Externo, c) Relaciones laborales y seguridad en el puesto de trabajo, d) Prácticas con clientes, productos defectuosos, e) Daños en activos materiales, f) Incidencias en el negocio y fallos en los sistemas, y g) Ejecución, entrega y gestión de procesos.

d) Principios de Basilea II para la administración del Riesgo Operativo

Los principios relacionados con la administración del riesgo operativo formulados por Basilea II en el marco adecuado para la gestión del riesgo, son los siguientes:

Desarrollo de un marco adecuado para la gestión del riesgo

Principio 1: El Consejo de administración⁴ deberá conocer cuáles son los principales aspectos de los riesgos operativos para el banco, en tanto que categoría de riesgo diferenciada, y deberá aprobar y revisar periódicamente el marco que utiliza el banco para la gestión de este riesgo. Este marco deberá ofrecer una definición de riesgo operativo válida para toda la empresa y establecer los principios para definir, evaluar, seguir y controlar o mitigar este tipo de riesgos.

Principio 2: El consejo de administración deberá asegurar que el marco para la gestión del riesgo operativo en el banco esté sujeto a un proceso de auditoría interna

eficaz e integral por parte de personal independiente, capacitado y competente. La función de auditoría interna no deberá ser directamente responsable de la gestión del riesgo operativo.

Principio 3: La alta gerencia deberá ser la responsable de poner en práctica el marco para la gestión del riesgo operativo aprobado por el consejo de administración. Dicho marco deberá ser aplicado de forma consistente en toda la organización bancaria y todas las categorías laborales deberán comprender sus responsabilidades al respecto. La alta gerencia también deberá ser responsable del desarrollo de políticas, procesos y procedimientos destinados a la gestión de estos riesgos para todos los productos, actividades, procesos y sistemas relevantes para el banco.

Gestión del riesgo: identificación, evaluación, seguimiento y cobertura/control

Principio 4: los bancos deberán identificar y evaluar el riesgo operativo inherente a todos sus productos, actividades, procesos y sistemas relevantes. Además, también deberán comprobar que antes de lanzar o presentar nuevos productos, actividades, procesos o sistemas, se evalúa adecuadamente su riesgo operativo inherente.

Principio 5: Los bancos deberán vigilar periódicamente los perfiles de riesgo operativo y las exposiciones sustanciales a pérdidas. La alta gerencia y el consejo de administración deberán recibir información pertinente de forma periódica que complemente la gestión activa del riesgo operativo.

Principio 6: Los bancos deberán contar con políticas, procesos y procedimientos para controlar y cubrir los riesgos operativos más relevantes. Además, deberán reexaminar periódicamente sus estrategias de control y reducción de riesgos y ajustar su perfil de riesgo operativo según corresponda, utilizando para ello las estrategias que mejor se adapten a su apetito por el riesgo y a su perfil de riesgo.

Principio 7: Los bancos deberán contar con planes de contingencia y de continuidad de la actividad, que aseguren su capacidad operativa continua y que reduzcan las pérdidas en caso de interrupción grave de la actividad.

La función de los supervisores

Principio 8: Los supervisores bancarios deberán exigir a todos los bancos, sea cual sea su tamaño, que mantengan un marco eficaz para identificar, evaluar, seguir y controlar o mitigar sus riesgos operativos más relevantes, como parte de su aproximación general a la gestión de riesgos.

Principio 9: Los supervisores deberán realizar, directa o indirectamente, una evaluación periódica independiente de las políticas, prácticas y procedimientos con los que cuentan los bancos para gestionar sus riesgos operativos. Además, deberán cerciorarse de que se han puesto en marcha los mecanismos necesarios para estar al tanto de cualquier novedad que se produzca en un banco.

La función de la divulgación de información

Principio 10: Los bancos deberán proporcionar información pública suficiente para que los partícipes del mercado puedan evaluar sus estrategias de gestión del riesgo operativo.

3. COSO Y LOS NUEVOS ENFOQUES DE LA EVALUACIÓN DE RIESGOS

a) COSO I

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

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

CAPITULO II Marco Conceptual, Teórico y Legal

se definen los lineamientos de control interno dependiendo del giro del negocio de cada organización.

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

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

Desde la primera definición del control interno establecida por el Instituto Americano de Contadores Públicos Certificados-AICPA que emite el documento denominado "Marco Integrado del Control Interno"(Internal Control – Integrated Framework). El Informe COSO, brinda el enfoque de una estructura común y/o estándar para comprender al control interno, el cual puede ayudar a cualquier entidad a alcanzar logros en su desempeño y en su economía, prevenir pérdidas de recursos, asegurar la elaboración de informes financieros confiables, así como el cumplimiento de las leyes y regulaciones, tanto en entidades privadas, como en públicas. COSO convierte los antiguos elementos de Control Interno en 5 componentes interrelacionados, que se derivan de la forma como la administración maneja el ente económico, y están integrados a los procesos administrativos:

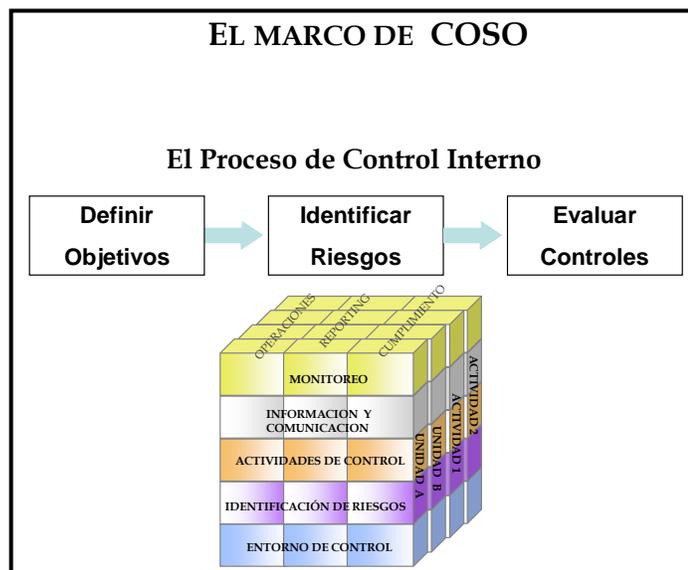


Figura 2 Marco de COSO

b) Componentes del COSO I

i. Ambiente de Control

El ambiente de control define al conjunto de circunstancias que enmarcan el accionar de una entidad desde la perspectiva del control interno y que son por lo tanto determinantes del grado en que los principios de este último imperan sobre las conductas y los procedimientos organizacionales.

ii. Evaluación de Riesgos

Con ella se establecen los objetivos institucionales y los riesgos asociados al logro de dichos objetivos, determinándose si los riesgos son gestionados adecuadamente, es decir, identificación, medición, monitoreo y control de los mismos.

iii. Actividades de control

Están constituidas por los procedimientos específicos establecidos como un reaseguro para el cumplimiento de los objetivos, orientados primordialmente hacia la prevención y neutralización de los riesgos.

iv. Información y comunicación

Así como es necesario que todos los funcionarios conozcan el papel que les corresponde desempeñar en la organización (funciones, responsabilidades), es imprescindible que cuenten con la información periódica y oportuna que deben manejar para orientar sus acciones en concordancia con los demás, hacia el mejor logro de los objetivos.

La información relevante debe ser captada, procesada y transmitida de tal modo que llegue oportunamente a todos los sectores permitiendo asumir las responsabilidades individuales.

v. Supervisión

Incumbe a la dirección la existencia de una estructura de control interno idónea y eficiente, así como su revisión y actualización periódica para mantenerla en un nivel adecuado. Procede la evaluación de las actividades de control de los sistemas a través del tiempo, pues toda organización tiene áreas donde los mismos están en desarrollo, necesitan ser reforzados o se impone directamente su reemplazo debido a que perdieron su eficacia o resultaron inaplicables. Las causas pueden encontrarse en los cambios internos y externos a la gestión que, al variar las circunstancias, generan nuevos riesgos a afrontar.

c) Marco de Control Interno Basado en Riesgos COSO ERM (COSO II)

Es la continuación del COSO I, fue emitido en 2004 es denominado por muchos COSO II, el cual provee un esquema más robusto y amplio de control al considerar

en el vasto campo del denominado “Risk Management” (Riesgos de Administración - Dirección) en las organizaciones.

Este modelo ha continuado trabajando en el esquema de control propuesto; ello, con el propósito público de apoyar a las organizaciones en el cumplimiento de sus objetivos, y los ha clasificado en cuatro categorías:

- Estratégica, por la importancia de su alineación con la misión.
- Operacional, en cuanto al uso eficaz y eficiente de recursos.
- De reporte, respecto a la confiabilidad de los reportes que se emitan.
- De cumplimiento, en cuanto al acatamiento de leyes y normatividad aplicable.

Según COSO II, los componentes del “control interno” se elevan a 8, en tanto que ya pasan a ser “componentes de la gestión de riesgos corporativos”.

La comparación entre el modelo COSO I y COSO II se muestra en la Figura 3 donde se advierte la relación entre los componentes de un modelo a otro.

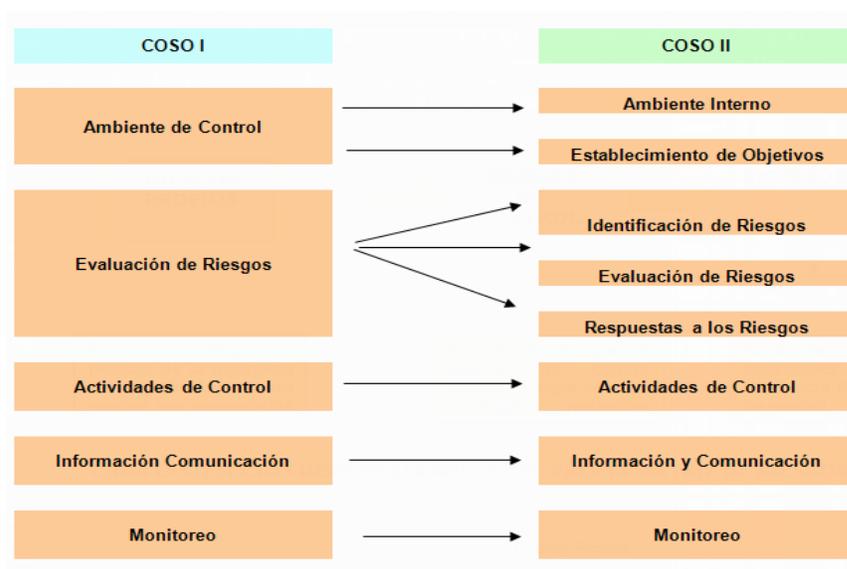


Figura 3 Relación entre COSO I y COSO II

De ese modo, un desarrollado “control interno” debe considerarse incluido en la actualidad en un nuevo marco suficientemente amplio para que, dentro de él y como uno de sus concretos componentes de la función gerencial, los directivos también practiquen eficazmente el “control de gestión” de las organizaciones que dirigen, en tanto que se enfatiza cómo asegurar el cumplimiento de objetivos, a través fundamentalmente de esa nueva conceptualización y desarrollo del marco integrado de la gestión de riesgos corporativos.

d) Definición de Gestión de Riesgos Corporativos COSO II ERM

Se define la “*gestión de riesgos corporativos*” como “*un proceso efectuado por el consejo de administración de una entidad, su dirección y restante personal, aplicado en la definición de la estrategia y en toda la entidad y diseñado para identificar eventos potenciales que puedan afectar a la organización y gestionar sus riesgos dentro del riesgo aceptado, proporcionando una seguridad razonable sobre el logro de objetivos*”.

Las finalidades de la Gestión de Riesgos son:

- Garantizar cumplimiento objetivos institucionales
- Fortalecer sistema de control interno
- Integrar riesgos en los procedimientos
- Asegurar cumplimiento de la Norma
- Hacer partícipes a los funcionarios en la prevención de los riesgos
- Evaluar los riesgos, reducirlos a través de controles efectivos para mantener la calidad de la gestión.

e) Componentes del COSO II – ERM

Los 8 componentes del E.R.M. están interrelacionados. Estos, se derivan de la manera como la administración opera un riesgo empresarial y están integrados dentro del proceso administrativo véase la Figura 4. Estos Componentes son:

i. Ambiente interno

El ambiente interno comprende el tono de una organización y establece las bases sobre cómo el riesgo es percibido y direccionado por la gente de una entidad, incluyendo la filosofía de la administración del riesgo y el apetito por el riesgo, la integridad y los valores éticos, y el ambiente en el cual operan.

ii. Establecimiento de objetivos

Este es uno de los nuevos componentes que COSO – ERM incorpora, y se refiere a que los objetivos tienen que existir antes de que la administración pueda identificar los eventos potenciales que afectan su logro. El E.R.M. asegura que la administración tiene en funcionamiento un proceso para establecer objetivos y que los objetivos seleccionados apoyan y están alineados con la misión de la entidad y son consistentes con su apetito por el riesgo.

iii. Identificación de eventos

Este es otro componente nuevo y establece que la Alta Dirección debe identificar los eventos internos y externos que afectan el logro de los objetivos de una entidad, diferenciando entre eventos y oportunidades. Las oportunidades se canalizan hacia la estrategia de la administración o hacia el proceso de establecimiento de objetivos.

iv. Evaluación de riesgos

Este es uno de los componentes nuevos más importantes dentro de la gestión de riesgo, porque establece que los riesgos se analizan, considerando su probabilidad e impacto, como una base para determinar cómo se deben administrar los riesgos. Los riesgos se valoran sobre una base inherente y una base residual.

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

v. Respuesta a los riesgos

Este es otro nuevo componente, que establece que la administración selecciona las respuestas al riesgo, es decir, evitar, aceptar, reducir, o compartir el riesgo, desarrollando un conjunto de acciones para alinear los riesgos con las tolerancias al riesgo y con el apetito por el riesgo que tiene la entidad.

vi. Actividades de control

Este componente desde el punto de vista del riesgo establece que la administración debe determinar e implementar políticas y procedimientos para ayudar a asegurar que las respuestas al riesgo se llevan a cabo de manera efectiva.

vii. Información y comunicación

Bajo este componente se resalta la necesidad de que exista información oportuna para una adecuada administración del riesgo, que le permita a la gente llevar a cabo sus responsabilidades. La comunicación efectiva también ocurre en un sentido amplio, fluyendo desde abajo, a través y hacia arriba de la entidad.

viii. Supervisión

Se monitorea la totalidad de la administración de riesgos del emprendimiento y se realizan las modificaciones necesarias. El monitoreo se logra mediante actividades administrativas ongoing, evaluaciones separadas o ambas.



Figura 4 Componentes COSO II – ERM

4. GUÍA PARA LAS NORMAS DEL CONTROL INTERNO DEL SECTOR PÚBLICO

La Guía para las Normas de control interno del sector público de 1992 de la INTOSAI (Organización Internacional de las Entidades Fiscalizadoras Superiores), fue concebida como un documento vital reflejando la visión que las normas pueden ser promovida para el diseño, implementación y la evaluación del control interno.

La 17ma Reunión de la INCOSAI (Seúl, 2001) reconoció una fuerte necesidad de actualizar la Guía de 1992 y acordó la utilización del marco integrado de control interno del Comité de Organizaciones que patrocinan la Comisión de Treadway (COSO). Consultas subsecuentes dieron resultados a una mayor extensión para tratar los valores éticos y proporcionar mayor información sobre los principios generales de las actividades del control relativos al tratamiento de la información.

La Guía actualizada para las normas de control interno fue emitida en el 2004, y puede ser considerada como un documento trascendental que debería ser desarrollado y perfeccionado continuamente para incorporar el impacto de nuevos avances como la Estructura de Manejo de Riesgo corporativo del COSO ERM. Por consiguiente, estas

extensiones a esta Guía han sido elaboradas para cubrir las tendencias actuales en la Administración de Manejo de Riesgos, según lo precisado en la estructura ERM del COSO. Siendo este documento dirigido principalmente para el sector público, el término "entidad" es utilizado en lugar de "corporación" que fue asociado particularmente al sector privado.

a) Definición de Gestión de Riesgos de la Entidad INTOSAI

Partiendo de que en el sector público los términos creación y preservación de valor no tienen directa relevancia como en el sector privado. Sin embargo, la definición es utilizada ampliamente con el propósito de aplicarse a todos los sectores y tipos de organizaciones que sea posible. En la medida de lo posible al sustituir la “creación y preservación de servicio” por la “creación o preservación de valor” esta terminología podrá ser plenamente aplicable en las entidades del sector público.

En este entendido, el COSO II que establece que la gestión de riesgos de la entidad, enfrenta riesgos y oportunidades afectando la creación de valores o la preservación de estos definidos de la siguiente manera:

"Gestión de riesgos de la entidad, es un proceso efectuado por la junta directiva de una entidad, la gerencia y el personal, que aplica en el planteamiento de la estrategia y a lo largo de la Entidad, está diseñado para identificar eventos potenciales que podrían afectar a la entidad y permite administrar el riesgo dentro de los límites aceptados, proveyendo la seguridad razonable para la consecución de objetivos de la entidad" (modelo 2004 de COSO ERM)

b) Gerencia de Riesgos de la Entidad - GRE

Es un modelo de gestión de riesgos denominado Gerencia de Riesgos de la Entidad GRE (ERM en inglés) que va más allá de las normas de control interno de la INTOSAI en un número de áreas, específicamente:

CAPITULO II Marco Conceptual, Teórico y Legal

- Las categorías de objetivos son más amplias, y también incluyen información más completa, información no financiera, objetivos estratégicos.
- Amplia el componente de evaluación de riesgos e introduce diversos conceptos del riesgo, tales como tendencia al riesgo, tolerancia del riesgo, respuesta al riesgo; y
- Acentúa la importancia de los directores independientemente en el directorio y elabora sus roles y responsabilidades.

Según la Guía INTOSAI, para implementar un sistema de gestión de riesgos de la entidad (GRE), debe considerarse lo siguiente:

Identificando la Misión

El punto de partida para la gestión de riesgos de la entidad es la misión y visión establecida por esta. Dentro del contexto de la misión, la entidad debería establecer los objetivos estratégicos, seleccionar las estrategias para alcanzar dichos objetivos y proponer objetivos de soporte alineados y desplegados en cascada a través de la organización.

Fijando Objetivos

La Guía para las Normas de control interno de la INTOSAI indica que los objetivos pueden ser subdivididos en cuatro categorías que son:

- **Estratégicos** – Metas de alto nivel, alineadas soportando la misión de la entidad.
- **Operacionales** – Orientados a la ejecución ordenada, ética, económica, eficiente y efectivamente de las operaciones; resguardando los recursos en contra de pérdidas, mal uso y daño.
- **Información** – Referido a que la información reportada incluyendo las obligaciones de contabilidad, la cual sea confiable.

CAPITULO II Marco Conceptual, Teórico y Legal

- **Cumplimiento** – Cumplimiento de leyes y regulaciones aplicables siendo posible actuar de acuerdo con la política gubernamental.

Los objetivos en las dos primeras categorías no están controlados por el control interno de la entidad, por lo que cualquier sistema de administración puede proporcionar solamente una razonable seguridad de que estos riesgos se manejan satisfactoriamente, pero debería permitir a la Dirección estar enterada del grado de cumplimiento oportuno de estos objetivos en un periodo de tiempo óptimo.

Sin embargo, los objetivos referentes a la confiabilidad de los reportes y cumplimiento están dentro del control de la entidad, por lo que la gestión efectiva de riesgos usualmente dará la seguridad de que estos objetivos serán alcanzados.

Identificando Eventos - Riesgos y Oportunidades

Una vez fijados los objetivos de la entidad, la gestión de riesgos requiere organizarse para identificar eventos que podrían tener impacto en el logro de los objetivos. Los eventos podrían tener impactos negativos o positivos o ambos a la vez. Los eventos con impacto negativo representan riesgos, los cuales podrían dificultar la habilidad de alcanzar los objetivos de una entidad. Estos riesgos pueden surgir debido a factores internos y externos.

Las oportunidades son la posibilidad de que la ocurrencia de un evento permita a la entidad alcanzar sus objetivos de manera más eficiente así como ver la posibilidad de mitigar los riesgos, la Gestión de riesgos de la entidad, podría permitir formular planes para identificar oportunidades.

Comunicación y aprendizaje

Determinar si la gestión de riesgos de la entidad, es “efectiva” es una parte fundamental del proceso. La gerencia necesita emitir un juicio acerca de si los componentes de la gestión de riesgos de la entidad, están presentes y operando efectivamente. Con mayor detalle que no existan debilidades materiales y que todos

CAPITULO II Marco Conceptual, Teórico y Legal

los riesgos hayan sido llevados dentro de los parámetros aceptables de la entidad. Cuando la gestión de riesgos es efectiva la gerencia comprende la extensión, en la cual los objetivos dentro de las cuatro categorías se han alineado con la misión y están siendo alcanzados. Una comunicación de arriba abajo y de abajo a arriba a través de la entidad es esencial para la facilitación de este proceso.

Limitaciones

Sin embargo, no importa cuán bien se haya diseñado y esté operando el sistema de gestión de riesgos de la entidad, esta no puede proveer a la entidad seguridad absoluta respecto al logro de los objetivos generales. En lugar de ello, este soporte reconoce que solo puede obtenerse un nivel razonable de seguridad.

La seguridad razonable se compara con un nivel satisfactorio de confianza de que los objetivos podrán ser alcanzados o que la gerencia podrá hacer conocer oportunamente si los objetivos probablemente no serán alcanzados. Determinar cuanta seguridad es requerida para alcanzar un nivel satisfactorio de confianza es tema de criterio. Al ejercitar esta decisión gerencial será necesario considerar los límites de riesgo de la entidad y los eventos que podrían impactar en el logro de los objetivos.

La seguridad razonable refleja la noción de que la incertidumbre y el riesgo se relacionan con el futuro, el cual nadie puede predecir con certeza. Además, los factores fuera del control o de la influencia de una entidad, tal como el factor político, pueden impactar la capacidad de alcanzar estos objetivos. En el sector público, los factores fuera del control de una entidad pueden incluso cambiar los objetivos centrales en un tiempo muy corto para saberlo. Las limitaciones también resultan de las siguientes realidades: el juicio humano en la toma de decisiones puede ser errado; crisis ocurridas debido a fallas humanas tales como errores simples o equivocaciones; que las decisiones en respuesta a un riesgo y controles establecidos necesitan considerar los costos relevantes y beneficios; y que los controles pueden

ser vulnerados por colusión entre dos o más personas y la gerencia puede anular el sistema de control.

Estas limitaciones impiden a la Entidad tener una seguridad absoluta de que los objetivos serán alcanzados. En la Figura 5 presenta algunos de los riesgos que se podrían enfrentar típicamente las entidades de los gobiernos. Intenta ser ilustrativo más que exhaustivo porque son los más comunes sin embargo no los únicos pueden existir otros riesgos que conforma a la tecnología y globalización puedan generarse o crearse.

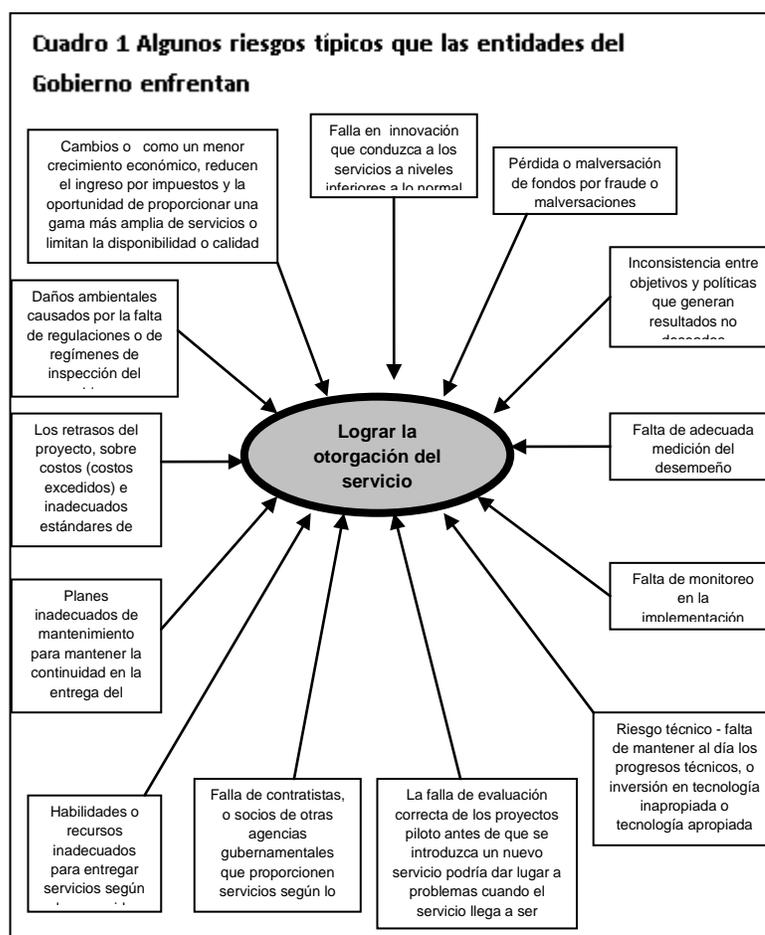


Figura 5 Riesgos que enfrentan los Gobiernos

Vínculo entre control interno y la gestión de riesgos de la entidad (GRE)

En muchos aspectos la gestión de riesgos de la entidad, puede ser vista como una evolución natural del modelo de control interno. La mayoría de las organizaciones intentarán aplicar completamente el modelo de control interno antes de implementar los conceptos inherentes a la gestión de riesgos de la entidad, el control interno es una parte integral de la gestión de riesgos.

El marco integrado de la gestión de riesgos de la entidad, involucra el control interno, formando una conceptualización y herramienta más robusta para la toma de decisiones respecto a posibles desvíos de su misión fundamental y objetivos asociados brindando una herramienta para la gerencia que le ayude a determinar cuál sería la respuesta correcta a un evento particular.

c) Componentes de la Gerencia de Riesgos de la Entidad

Al igual que el COSO II, Gerencia de Riesgos de la Entidad, consta de ocho componentes interrelacionados. Éstos fueron derivados de la manera como la administración lleva a cabo un negocio y fueron integrados con el proceso de gestión. Los componentes son:

- Ambiente de Riesgo/Contexto
- Establecimiento de objetivos
- Identificación de eventos
- Evaluación de riesgos
- Respuesta a los riesgos
- Actividades de control
- Información y comunicación
- Monitoreo

En la aplicación de los componentes de la gestión de riesgos, de la entidad, ésta debería considerar todos los alcances de sus actividades en todos los niveles de la

organización. La administración debería también considerar nuevas iniciativas y proyectos usando el marco de trabajo de la gestión de riesgos de la entidad (GRE).

Aplicando la gestión de riesgos a toda la entidad

La gerencia requiere adoptar una perspectiva según el portafolio de riesgos. En efecto todos los mandos medios de la gerencia necesitarán considerar los eventos que pueden impactar sus áreas de actividad y alimentar con los mismos a la gerencia superior. Esta evaluación puede ser cualitativa o cuantitativa. La gerencia superior debe utilizar estas evaluaciones a través de todos los niveles y áreas de negocios de la entidad para construir un nivel medio para de evaluación general del portafolio de riesgos de la organización.

Importancia de las personas

La gestión de riesgos de la entidad, es implementada y puesta en marcha efectiva por la gerencia y otro personal lograda por las personas dentro de la organización mediante lo que hacen y dicen; de similar forma, afecta a las acciones de las personas debido a que cada empleado es una persona con diferente forma de entender y competencias. Asimismo, la GRE trata de proporcionar los mecanismos necesarios para permitir a los miembros del directorio a entender el riesgo en el contexto de los objetivos de la entidad.

Los miembros del directorio deben conocer sus responsabilidades y los límites de su autoridad. Por este motivo deberá existir un vínculo claro y conciso entre los deberes de las personas y el modo de realizarlos. La gerencia superior principalmente proporciona un asesoramiento. Sin embargo, ellos también proporcionan directrices, aprueban estrategias y ciertas transacciones y políticas de forma que desempeñen un papel importante en el fortalecimiento de la cultura organizacional.

5. NORMA AS/NZS 4360: 2004 DE ADMINISTRACIÓN DE RIESGOS

El estándar de administración de riesgos AS/NZS 4360 publicado por primera vez en 1999, ha sido revisado y emitido como AS/NZS 4360:2004 en la gestión 2004, este documento suministra orientaciones genéricas para la gestión de riesgos. Puede aplicarse a una gran variedad de actividades, decisiones u operaciones de cualquier entidad pública, privada o comunitaria, grupos o individuos. Se trata de un modelo amplio, que permite la definición de objetivos específicos de acuerdo con las necesidades de implementación. La aplicación de esta norma garantiza a toda organización una base sólida para la aplicación de cualquier otra norma o metodología de gestión de riesgos específica para un determinado segmento.

Especifica los elementos del proceso de administración de riesgos, siendo genérico e independiente de cualquier industria o sector. El diseño e implementación de un sistema de administración de riesgo dependerá de las necesidades de cada organización, sus objetivos particulares, sus productos, servicios y procesos.

Debe aplicarse en todas las etapas de vida de una actividad, función, proyecto, producto o activo. El mayor beneficio es obtenido cuando se aplica desde el inicio.

El objetivo del estándar es brindar una guía que permita, tanto a las organizaciones públicas o privadas, grupos o individuos, alcanzar lo siguiente:

- Una base confiable y rigurosa para el planeamiento y toma de decisiones.
- Efectiva identificación de oportunidades y amenazas.
- Administración proactiva antes que reactiva.
- Mejor distribución y uso de los recursos.
- Confianza de los “stakeholders”.
- Cumplimiento con aspectos regulatorios cuando esto aplique.
- Mejor Gobierno Corporativo.

a) Definiciones de la Administración de Riesgos de la AS/NZS 4360:2004

A continuación se presentan algunas definiciones importantes a tener en cuenta en relación a la administración de riesgos, dentro de estas son:

- Consecuencia: impacto de un evento.
- Control: proceso, política, dispositivo, práctica o cualquier otra acción que actúa para minimizar un riesgo o ampliar oportunidades.
- Evaluación de controles: revisión sistemática de los procesos para asegurar que los controles continúen siendo efectivos y apropiados. La periodicidad de la evaluación de los controles la establece cada organización de acuerdo a la naturaleza de sus negocios y/o objetivos.
- Evento: ocurrencia de un conjunto particular de circunstancias. El evento puede tener una sola ocurrencia o convertirse en una cadena.
- Frecuencia: medida del número de ocurrencias por unidad de tiempo.
- Amenaza: fuente potencial de algún daño o desperfecto.
- Probabilidad: usada como una descripción general de la frecuencia de ocurrencia. Puede expresarse cualitativamente o cuantitativamente.
- Pérdida: cualquier consecuencia negativa o efecto adverso, financiero o de otro tipo que daña a la organización. El daño a la imagen de la organización puede incluirse como una pérdida.
- Monitoreo: consiste en la verificación, supervisión del progreso de una actividad, acción o sistema con la finalidad de identificar cambios en el desempeño, de acuerdo a los niveles previamente establecidos.
- Organización: grupo de personas e instalaciones, con responsabilidades, autoridad y relaciones.

CAPITULO II Marco Conceptual, Teórico y Legal

- Riesgo: posibilidad de que ocurra algo que pueda tener algún tipo de impacto en los objetivos de una organización. Generalmente es expresado en términos de un evento o circunstancia y las consecuencias que puede producir.
- Riesgo Residual: es el riesgo que permanece luego de haber implementado un control o tratamiento.
- Análisis de Riesgos: proceso sistemático que consiste en entender la naturaleza de los riesgos y deducir su nivel.
- Administración de Riesgos: consiste en el proceso de identificación, análisis y evaluación de riesgos.
- Eliminación de riesgo: decisión que se toma en función a la situación que presenta el origen del riesgo.
- Criterios para un riesgo: términos de referencia que son tomados en cuenta al evaluar un riesgo. Se refiere a costos y beneficios asociados, requerimientos legales y regulatorios, requerimientos de usuarios, etc.
- Evaluación de riesgos: proceso de comparar los niveles de riesgo con los criterios previamente establecidos.
- Identificación de riesgos: proceso para determinar qué, dónde, cuándo, por qué y cómo podría ocurrir algo.
- Proceso de Administración de riesgos: aplicación sistemática de políticas, procedimientos y prácticas en las tareas de comunicación, establecimiento del contexto, identificación, análisis, evaluación, tratamiento, monitoreo y revisión de riesgos.
- Plataforma para la administración de riesgos: conjunto de elementos que forman parte del sistema de gestión de una organización en relación a la administración

CAPITULO II Marco Conceptual, Teórico y Legal

de riesgos. Estos elementos pueden incluir planeamiento estratégico, estrategias, toma de decisiones y cualquier proceso o práctica que maneje los riesgos.

- **Retención del riesgo:** intencionalmente o sin intención retener la responsabilidad por las pérdidas, o la carga financiera de las pérdidas dentro de la organización. La retención del riesgo también incluye los riesgos que no han sido identificados.
- **Compartir el riesgo:** se comparte el riesgo con un tercero fuera de la organización. Generalmente se habla de transferir el riesgo, y lo usual es a través de seguros.
- **Tratamiento de riesgos:** proceso de selección e implementación de medidas o controles para atenuar el impacto negativo de un riesgo.

b) Elementos del proceso de Administración de Riesgos AS/NZS 4360: 2004

Los principales elementos en el proceso de administración de riesgos según el estándar australiano son:

- **Establecer el contexto:** referido a la estrategia, organización y administración de riesgos en el cual tendrá lugar el resto del proceso. Se deben establecer aquellos criterios o métricas contra los cuales se evaluarán los riesgos.
- **Identificar riesgos:** se deben identificar los riesgos que se pretenda gestionar. Para ello debe efectuarse un análisis de los principales procesos de negocio de la organización, en especial, de aquellos que pueden catalogarse como los más críticos para el normal funcionamiento de la organización. Es importante detectar todas aquellas vulnerabilidades a las que está expuesta la organización, para luego identificar aquellas amenazas que pueden aprovecharlas.
- **Analizar los riesgos:** se identifican los controles implementados para atenuar los riesgos, con la finalidad de establecer si continúan funcionando de manera adecuada. Como parte del análisis deben evaluarse las probabilidades de ocurrencia

CAPITULO II Marco Conceptual, Teórico y Legal

y los impactos de cada uno de los riesgos para luego establecer su nivel y esto permita realizar una priorización.

- **Evaluar riesgos:** se comparan los niveles de riesgo obtenidos contra las métricas o criterios preestablecidos. Cada organización de acuerdo a sus objetivos y políticas decidirán el orden de atención de los mismos, usando como base el nivel obtenido a partir de las métricas.
- **Tratar riesgos:** en relación a aquellos riesgos que tengan un nivel bajo o aceptable, estos se atenderán con procedimientos de rutina normales dentro de los procesos de negocio de la organización. Para los riesgos con un mayor nivel, se deben desarrollar e implementar medidas que logren en lo posible ponerlos en nivel aceptable para la organización.
- **Monitoreo y revisión:** se debe realizar periódicamente una medición del desempeño de los controles implementados, pues podría darse el caso que en algún momento éstos necesiten ser mejorados, complementados o incluso cambiados.
- **Comunicar y Consultar:** se debe mantener una comunicación constante con los dueños de los procesos de negocio en una organización, pues finalmente ellos son los más indicados para dar un juicio de los controles implementados para tratar los riesgos a los que se ven expuestos.

En la Figura 6 se muestra gráficamente el proceso de administración de riesgos

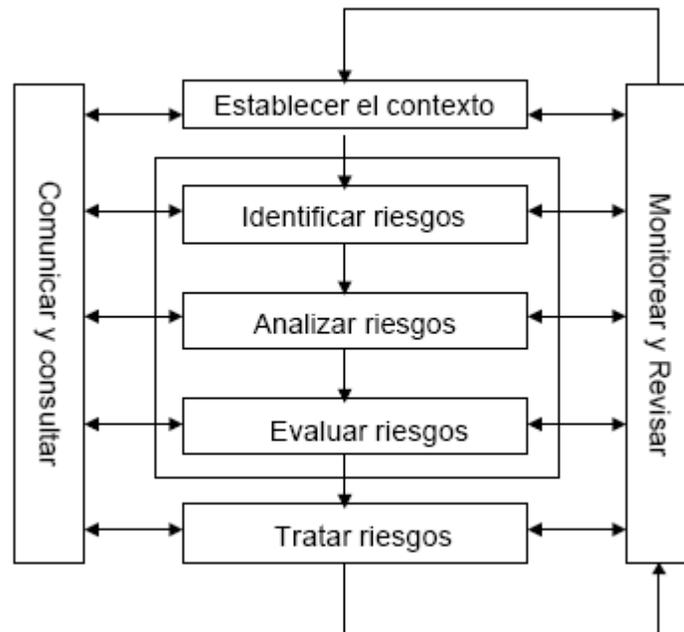


Figura 6 Proceso de Administración de Riesgos

En relación a la administración de riesgos se presentan algunos tipos de éstos a los que se ven expuestos la mayoría de organizaciones. De acuerdo al tipo de organización, uno o más de los siguientes riesgos pueden presentarse:

- **Riesgo Estratégico:** Se asocia con la forma en que se administra la organización. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la organización por parte de la alta gerencia.
- **Riesgos Operativos:** Comprende los riesgos relacionados tanto con la parte operativa como técnica de la organización, incluye riesgos provenientes de deficiencias en los sistemas de información, en la definición de los procesos, en la estructura de la organización, la desarticulación entre dependencias lo cual conduce a ineficiencias, oportunidades de corrupción e incumplimiento de los compromisos institucionales.

CAPITULO II Marco Conceptual, Teórico y Legal

- **Riesgos de Control:** Están directamente relacionados con inadecuados o inexistentes puntos de control y en otros casos, con puntos de controles obsoletos, inoperantes o poco efectivos.
- **Riesgos Financieros:** Se relacionan con el manejo de los recursos de la organización que incluye, la ejecución presupuestal, elaboración de los estados financieros, pagos, manejos de excedentes de tesorería y el manejo sobre los bienes de cada organización. De la eficiencia y transparencia en el manejo de los recursos, así como su interacción con las demás áreas dependerá en gran parte el éxito o fracaso de toda organización.
- **Riesgos de Cumplimiento:** Se asocian con la capacidad de la organización para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la los entes reguladores.
- **Riesgos de Tecnología:** Se asocia con la capacidad de la organización para satisfacer sus necesidades actuales y futuras, así como para soportar el cumplimiento de su misión a través de su tecnología disponible.

El análisis de riesgos se puede desarrollar en distintos niveles de detalle dependiendo del tipo de riesgo, propósito del análisis, y sobre todo de la disponibilidad de información, datos y recursos. El análisis puede ser cualitativo, semi-cuantitativo, cuantitativo, o una combinación de estos dependiendo de las circunstancias. El orden de complejidad y costos de análisis, en orden ascendente, es cualitativo, semi-cuantitativo y cuantitativo.

En la práctica el análisis cualitativo es usado con frecuencia para obtener un esquema general de los riesgos a los que está expuesta una organización. A partir de este punto, si se desea entrar en detalles, se utilizará el análisis cuantitativo, siendo necesario contar con datos históricos correctamente cuantificados. Esto puede lograrse implementando las llamadas base de datos de pérdidas.

Daremos a continuación algunos lineamientos en relación a los tipos de análisis de riesgos mencionados:

- **Análisis Cualitativo:** emplea palabras para describir la magnitud de las potenciales consecuencias y probabilidad de ocurrencia de las mismas. Las escalas a emplearse pueden ser adaptadas de acuerdo a las circunstancias, y pueden emplearse distintas descripciones según el tipo de riesgo. Las escalas más frecuentes en uso son las probabilidades y consecuencias bajos, medios y altos. La combinación de los pares nos dan como resultado el nivel de riesgo.

El análisis cualitativo puede ser usado como:

- Una primera actividad de reconocimiento de riesgos a los que está expuesta una organización. Este primer reconocimiento constituirá la base para un posterior análisis más detallado.
- Apoyo en la toma de decisiones
- Alternativa cuando no se cuenta con datos numéricos históricos o recursos suficientes para un análisis cuantitativo.
- **Análisis Semi-Cuantitativo:** En este tipo de análisis se busca ampliar la escala del análisis cualitativo, asignando valores numéricos iniciales, con cierta aproximación. Esto sentará una mejor base para el análisis cuantitativo, en el cual los valores numéricos serán más exactos. Es importante asignar con cuidado los valores a las probabilidades de ocurrencia de los eventos de riesgo, pues esto puede dar resultados inexactos, los cuales no reflejen la verdadera situación de los niveles de riesgo de la organización.
- **Análisis Cualitativo:** Este análisis emplea valores numéricos (a diferencia de escalas descriptivas usadas en el análisis cualitativo y semi-cualitativo) tanto para las probabilidades e impactos, empleando datos de varias fuentes (base de datos de pérdida por ejemplo). La precisión del análisis dependerá mucho de la exactitud y veracidad de los datos obtenidos de las fuentes que se consulten. Los impactos de

CAPITULO II Marco Conceptual, Teórico y Legal

los riesgos generalmente se expresarán en términos monetarios. En algunas oportunidades quizás se obtendrán distintos valores en el análisis para un sólo evento, esto de acuerdo a cómo ha ido variando el tiempo.

La forma en cómo se expresen las probabilidades e impactos y cómo se combinen para obtener un nivel de riesgo podrá variar de acuerdo al tipo de éste y del propósito del análisis de riesgos. Este es un documento que describe una metodología de administración de riesgos genérica aplicable a cualquier entidad sea pública o privada.

6. ISO 31000 GESTIÓN DE RIESGOS

Debido a los acontecimientos económicos recientes, todo indica que contar con una capacidad adecuada para gestionar los riesgos en las organizaciones hoy es un factor clave y diferenciador, ya sea en empresas y servicios públicos, instituciones privadas o bien en organizaciones sin fines de lucro o gubernamentales.

Sus antecedentes están en el modelo FERMA 2003 y en normas como la australiana/neo zelandesa AS/NZS 4360

En noviembre del 2009 la Organización Internacional para la Estandarización (International Organization for Standardization – ISO -) publicaba la ISO 31000:2009 (Gestión de Riesgos: Principios y Directrices), con el objetivo de ayudar a las organizaciones, independientemente del tipo y tamaño que éstas posean, a gestionar sus riesgos de manera eficaz, eficiente y coherente. Esta norma se convierte en el primer estándar en establecer un marco general sobre el que desarrollar los procesos de gerencia de riesgos y consta de cinco cláusulas y un anexo.

Hasta la aprobación de la ISO 31000 sólo se disponía de modelos ‘ad-hoc’ de uso específico para ciertas actividades: COSO, Basilea, Solvencia, UNE 150008, así como algún otro modelo de carácter integral de Risk Management entre ellos, el mencionado modelo FERMA o la norma australiana-neo zelandesa AS/NZS 4360:2004.

Esta norma proporciona instrucciones sobre cómo establecer y mantener un marco de gestión de riesgos de carácter oficial que puede ser adoptada por cualquier organización. Aunque esta norma proporciona directrices genéricas, no es su intención promover la uniformidad de la gestión de riesgo a través de las compañías, ya que, se entiende que el diseño y ejecución de un modelo de gestión de riesgos y los marcos de referencia deben tener en cuenta las diversas necesidades de una organización específica, sus objetivos estratégicos particulares, el contexto, su estructura, volumen de operaciones, procesos, funciones, proyectos, productos, servicios o activos específicos y las prácticas empleadas.

El enfoque recogido en la ISO 31000 está estructurado sobre la base de tres elementos claves para conseguir una gestión de riesgos efectiva: los principios para la gestión de riesgos; la estructura de soporte y el proceso de gestión de riesgos. La relación entre los tres principios: gestión, estructura y procesos se muestra en la Figura 7 en un esquema sintético.

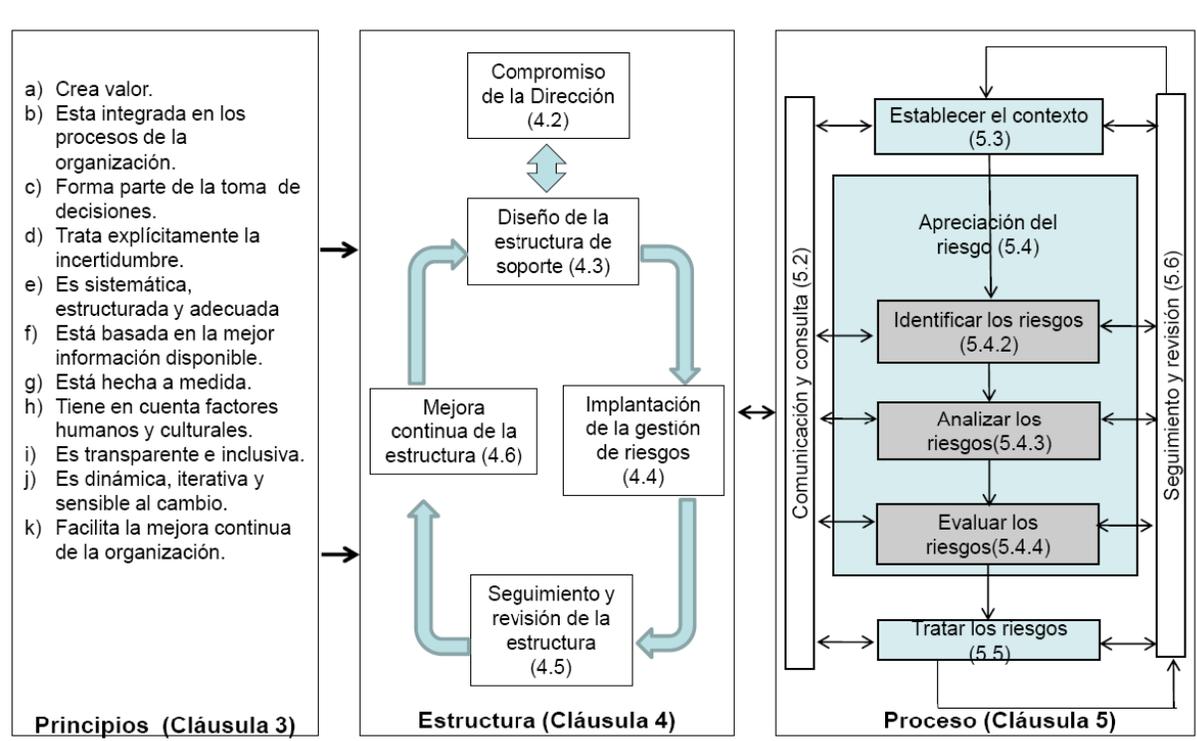


Figura 7 Esquema de la Relación entre los Principios, Estructura y Proceso

a) Definiciones de la Gestión de Riesgos ISO 31000

La ISO 31000:2009 ha incorporado conceptos adicionales al estándar Australiano Neozelandés AS/NZS 4360:2004 y entre sus principios más importantes se encuentran los siguientes:

- Define el riesgo como **un efecto de incertidumbre en el logro de los objetivos**
- Los principios que recomienda a seguir por las organizaciones son más explícitos que su antecesor AS/NZS 4360:2004.

- Aconseja integrar en forma explícita el mejoramiento continuo de la estructura de administración de riesgo.
- Incorpora la necesidad de contar con la integración de elementos principalmente como: gobierno, estrategia y planificación, políticas, valores y la cultura de la organización.

b) Principios de la Gestión de Riesgos

La norma ISO 31000 a diferencia de la norma AS/NZS 4360:2004 establece principios para la gestión de riesgo, que tienen que ser aplicados en todos los niveles de una organización de acuerdo a lo siguiente:

i. La gestión de riesgo crea y protege el valor.

La gestión del riesgo contribuye a la consecución de los objetivos y demostrables de mejora del rendimiento por ejemplo, la salud humana y la seguridad, la seguridad, jurídica y el cumplimiento regulatorio, publico la aceptación, la protección del medio ambiente, la calidad del producto, gestión de proyectos, la eficiencia en las operaciones, la gobernanza y la reputación.

ii. Es una parte integral de todos los procesos de organización.

La gestión de riesgos no es una actividad aislada, separada de las principales actividades y procesos de la organización. La gestión de riesgos es parte de las responsabilidades de gestión y como parte integrante de todos los procesos de organización, incluida la planificación estratégica y de todos los proyectos y la gestión del cambio procesos.

iii. La gestión de riesgos es parte de la toma de decisiones.

La gestión de riesgos ayuda a quienes toman las decisiones, priorizar acciones y distinguir entre cursos alternativos de acción.

iv. Aborda explícitamente la incertidumbre.

La gestión de riesgos tiene en cuenta explícitamente la incertidumbre, la naturaleza de esa incertidumbre, y como se puede dirigir.

v. La gestión de riesgo es sistemática, estructurada y oportuna.

Un enfoque sistemático, oportuno y estructurado para la gestión del riesgo contribuye a la eficiencia y para resultados consistentes, comparables y fiables.

vi. Se basa en la mejor información disponible.

Las entradas para el proceso de gestión de riesgo se basan en fuentes de información como los datos históricos, la experiencia, información de los interesados, la observación, pronósticos y opiniones de expertos. Sin embargo, la decisión los responsables deben informarse, y debe tener en cuenta las limitaciones de los datos o de modelos utilizados o la posibilidad de divergencia entre los expertos.

vii. La gestión del riesgo es la medida.

La gestión del riesgo se alinea con el contexto e interno de la organización y perfil de riesgo.

viii. La gestión del riesgo tiene los factores humanos y culturales en cuenta.

La Gestión del riesgo reconoce las capacidades, las percepciones y las intenciones de las personas internas y externas que puede facilitar u obstaculizar el logro de los objetivos de la organización

ix. La gestión del riesgo sea transparente e inclusivo.

Adecuado y la oportuna participación de los interesados y, en particular, los tomadores de decisiones en todos los niveles de la organización, asegura que la gestión del riesgo sigue siendo pertinente y actualizada. También permite la participación de las partes interesadas estén debidamente representados y que sus opiniones sean tenidas en la determinación del riesgo criterios.

x. **La gestión de riesgos es dinámica, interactiva y de respuesta al cambio.**

La gestión de riesgos continuamente sentidos y responde a los cambios. Como los acontecimientos externos e internos ocurren, el contexto y el cambio de conocimiento, seguimiento y revisión de los riesgos de tener lugar, surgen nuevos riesgos, algunos el cambio, y otras desaparecen.

xi. **La gestión de riesgos facilita la mejora continua de la organización.**

Las organizaciones deben desarrollar y aplicar estrategias para mejorar su madurez de gestión de riesgos junto con todos los demás aspectos de su organización.

c) **Marco de Gestión del Riesgo**

El éxito de la gestión de riesgo dependerá de la eficacia del marco de gestión que proporciona las bases y disposiciones que incrustarlo en toda la organización en todos los niveles. El marco ayuda en la gestión de los riesgos de manera efectiva a través de la aplicación del proceso de gestión del riesgo en los diferentes niveles y dentro de los contextos específicos de la organización. El marco garantiza que la información sobre los riesgos derivados del proceso de gestión está adecuadamente informada y se utiliza como base para la toma de decisiones y la rendición de cuentas en todos los niveles pertinentes de organización. Esta cláusula se describe los componentes necesarios del marco para la gestión del riesgo y la manera en que se interrelacionan de manera iterativa, como se muestra en la Figura 8.

Este marco no tiene por objeto establecer un sistema de gestión, sino más bien pretende ayudar a la organización a integrar a la gestión de riesgos en su sistema de gestión global. Por lo tanto, las organizaciones deben adaptar los componentes del marco de acuerdo a sus necesidades específicas.

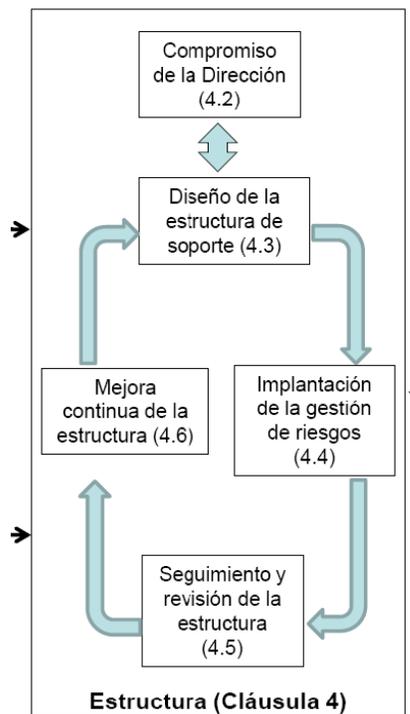


Figura 8 Marco de la Gestión del Riesgo

i. Mandato y el compromiso (4.2)

La introducción de la gestión del riesgo en la entidad y asegurar su eficacia permanente, requiere un fuerte y sostenido compromiso por parte de la Alta Dirección de las entidades en cuanto a la gestión integral, así como la planificación estratégica y objetivos a alcanzar con el compromiso en todos los niveles. La dirección debería:

- Definir y aprobar la política de gestión de riesgos;
- Garantizar que están alineados la cultura de la organización y la política de gestión de riesgos;
- Determinar los indicadores de gestión de riesgo de cumplimiento que se alinean con los indicadores de rendimiento de la organización;
- Alinear los objetivos de gestión del riesgo con los objetivos y estrategias de la organización;

CAPITULO II Marco Conceptual, Teórico y Legal

- Garantizar el cumplimiento legal y reglamentario;
- Asignar responsabilidades y las responsabilidades en los niveles apropiados dentro de la organización;
- Garantizar que los recursos necesarios destinados a la gestión de riesgos;
- Comunicar los beneficios de la gestión de riesgos a todos los interesados
- Garantizar que el marco para la gestión del riesgo sigue siendo apropiado

ii. Diseño del marco para la gestión de riesgo (4.3)

• Comprensión de la organización y su contexto (4.3.1)

Antes de iniciar el diseño y la aprobación del marco para la gestión de riesgos, es importante evaluar y entender tanto el contexto externo e interno de la organización, ya que estos pueden reducir significativamente o influir en el diseño del marco.

Evaluación de contexto externo de la organización puede incluir, pero no se limita a:

- a) Culturales y sociales, legales, regulatorios, financieros, tecnológicos, económicos, desarrollo competitivo y natural, medio ambiente, ya sea internacional, nacional, regional o local;
- b) Principales factores y tendencias que tienen un impacto sobre los objetivos de la organización, y
- c) Relaciones, percepciones y evaluaciones de, los actores externos.(stakeholders)

Evaluación de contexto interno de la organización puede incluir, pero no se limita a:

- Gobernanza, la estructura organizativa, las funciones y responsabilidades;

CAPITULO II Marco Conceptual, Teórico y Legal

- Las políticas, los objetivos y las estrategias que están en marcha para alcanzarlos;
 - Capacidades, entendida en términos de recursos y conocimientos (capital, por ejemplo, tiempo, personas, procesos, sistemas y tecnologías);
 - Los sistemas de información, flujos de información y la toma de decisiones (tanto formales como informales);
 - Relaciones con, y las percepciones y los valores de grupos de interés internos;
 - Cultura de la organización;
 - Normas, directrices y modelos adoptados por la organización, y
 - La forma y el alcance de las relaciones contractuales
- **Establecimiento de la política de gestión de riesgos(4.3.2)**

La política de gestión de riesgos debe exponer claramente en los objetivos de la organización y su compromiso, la gestión del riesgo mínimamente abordara los siguientes temas:

- Fundamentos de la organización para la gestión de riesgos
- Vínculos entre los objetivos de la organización y las políticas de gestión de riesgos;
- Rendición de cuentas y Responsabilidades para la gestión de riesgos;
- La forma en que los intereses en conflicto son tratados
- Compromiso obtener los recursos necesarios para ayudar a los responsables de la gestión de riesgo;
- La forma en que los resultados de la gestión de riesgo serán medidos y reportados, y
- El compromiso de revisar y mejorar la política de gestión del riesgo y el marco periódicamente y en respuesta a un suceso o cambio en las circunstancias.

La política de gestión de riesgos debe ser comunicada apropiadamente.

- **Rendición de cuentas (4.3.3)**

La organización debe garantizar que haya rendición de cuentas, la autoridad y las competencias adecuadas para la gestión del riesgo, incluyendo la implementación y el mantenimiento del proceso de gestión de riesgo y garantizar la adecuación, eficacia y eficiencia de los controles. Esto puede ser facilitado mediante:

- La identificación de los dueños de los riesgos que tienen la responsabilidad y la autoridad para gestionar riesgos;
- Identificar quien es el responsable de la elaboración, aplicación y mantenimiento del marco para la gestión de riesgo;
- Otras responsabilidades identificadas de las personas en todos los niveles en la organización para la gestión del riesgo de los procesos;
- El establecimiento de la medición del desempeño y presentación de informes externos y / o internos y el aumento de los procesos; y
- Garantizar niveles adecuados de reconocimiento.

- **Integración en los procesos de organización (4.3.4)**

Gestión de riesgos debe estar integrada en todas las prácticas de la organización y los procesos de una manera que sea relevante, eficaz y eficiente. El proceso de gestión de riesgos debe formar parte de y no separada de los procesos de organización.

Debe haber un plan de riesgos en toda la organización para asegurar que la política de gestión de riesgos sea implementado y que la gestión de riesgos está integrada en todas las prácticas de la organización y procesos. El plan de gestión de riesgos puede ser integrado en otros planes de la organización, tales como el plan estratégico.

- **Recursos (4.3.5)**

La organización debe asignar los recursos adecuados para la gestión de riesgos. Se debe considerar lo siguiente:

- Las personas, habilidades, experiencia y competencia;
- Los recursos necesarios para cada etapa del proceso de gestión de riesgos;
- Procesos de la organización, métodos y herramientas que se utilizan para la gestión de riesgos;
- Los procesos y procedimientos documentados;
- La información y los sistemas de gestión del conocimiento, y
- Programas de formación y capacitación.

- **El establecimiento de mecanismos de comunicación interna y la presentación de informes (4.3.6)**

La organización debe establecer la comunicación interna y mecanismos de información a fin de apoyar y de fomentar la rendición de cuentas y la titularidad de riesgo. Estos mecanismos debería garantizar que:

- Componentes clave del marco de gestión de riesgos, y cualquier modificación posterior, se comunica apropiadamente;
- Hay informes internos adecuados sobre el marco, su eficacia y los resultados;
- La información pertinente derivada de la aplicación de gestión de riesgo es en los niveles adecuados y los tiempos,
- Hay procesos de consulta con las partes interesadas (stakeholders).

Estos mecanismos deberían, en su caso, incluyen los procesos para consolidar la información de riesgo de una variedad de fuentes, y puede tener en cuenta la sensibilidad de la información.

- **Establecimiento de mecanismos para la comunicación externa y la presentación de informes (4.3.7)**

La organización debe desarrollar e implementar un plan de cómo va a comunicarse con su entorno externo y las partes interesadas. Esto implica:

- Involucrar a los interesados externos adecuados y garantizar un intercambio eficaz de información;
- Presentación de informes externos para cumplir con los requisitos legales, reglamentarios y de gobierno;
- Proporcionar retroalimentación e informes sobre la comunicaciones consultas;
- Utilizar la comunicación para fomentar la confianza en la organización, y
- La comunicación con las partes en el caso de una crisis o de emergencia.

Estos mecanismos deberían ser incluidos en los procesos para consolidar la información de riesgo, de una variedad de fuentes, teniendo en cuenta su sensibilidad.

iii. Implementando la gestión de riesgos (4.4)

- **Aplicación del marco para la gestión del riesgo (4.4.1)**

En la aplicación del marco de la organización para la gestión de riesgos, la organización debería:

- Definir el momento oportuno y la estrategia para la aplicación del marco;
- Aplicar la política de gestión de riesgos y el proceso de los procesos de organización;
- Cumplir con los requisitos legales y reglamentarios;
- Garantizar que la toma de decisiones, incluyendo el desarrollo y establecimiento de objetivos, está alineado con los resultados de los procesos de gestión de riesgos;
- Celebrar sesiones de información y formación, y

- Comunicación y consulta con las partes interesadas para asegurarse de que su marco de gestión del riesgo sigue siendo adecuado.

- **La implementación del proceso de gestión de riesgos (4.4.2)**

La gestión del riesgo, debe aplicarse para garantizar que el proceso de gestión del riesgo descrito en la cláusula 5 (del documento original ISO 31000), se aplica a través de un plan de gestión de riesgos en todos los niveles y funciones pertinentes de la organización como parte de sus prácticas y procesos.

iv. Seguimiento y revisión del marco (4.5)

Con el fin de garantizar que la gestión de riesgos es eficaz y este sigue apoyando el desempeño organizacional, la organización debe:

- Medir el desempeño de la Gestión de Riesgos con indicadores de gestión, que son periódicamente revisados para pertinencia;
- Periódicamente medir los progresos, las desviaciones respecto del plan de gestión de riesgos;
- Revisar periódicamente si el marco de la gestión de riesgos, la política y el plan siguen siendo pertinentes, teniendo en cuenta el contexto externo e interno de las organizaciones;
- Informe sobre el riesgo, el progreso respecto del plan de gestión de riesgos y lo bien que la política de gestión de riesgo se está siguiendo,
- Revisar la eficacia del marco de gestión de riesgos.

v. La mejora continua del marco (4.6)

Basándose en los resultados de la vigilancia y opiniones, las decisiones deben tomarse sobre la forma del marco de la gestión del riesgo, la política y el plan de gestión de riesgos puede ser mejorado. Estas decisiones deben conducir a mejoras en la organización sobre la gestión y la cultura de gestión del riesgo.

d) Proceso de Gestión del Riesgo

El proceso de gestión del riesgo debe ser

- Una parte integral de la gestión,
- Arraigados en la cultura y las prácticas,
- Adoptados a los procesos de negocio de la organización.

Comprende las actividades descritas en 5,2 a 5,6 del documento ISO 31000:2009.

El proceso de gestión de riesgos se muestra en la figura 9.

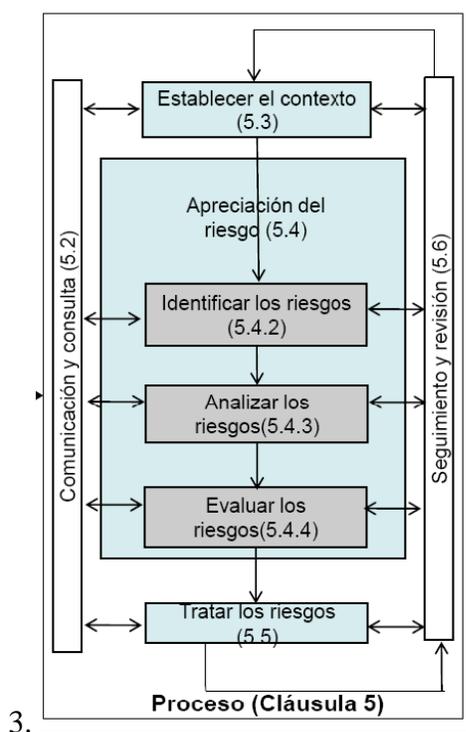


Figura 9 Relación entre los procesos

i. Comunicación y consulta

Comunicación y consulta con las partes interesadas externas e internas debería tener lugar durante todas las etapas del proceso de gestión de riesgos.

Por lo tanto, los planes de comunicación y consulta deben desarrollarse en una etapa temprana. Estos deben abordar las cuestiones relacionadas con el riesgo en sí mismo, sus causas, sus consecuencias (si se conoce), y las medidas que se adoptan para tratarla. La comunicación interna y externa efectiva y la consulta debe llevarse a cabo para garantizar que los responsables de la aplicación del proceso de gestión del riesgo y las partes interesadas a entender la base en la que se toman las decisiones, y las razones particulares por las medidas necesarias.

ii. Establecer el contexto: (5.3)

Al establecer el contexto, la organización articula sus objetivos, define el entorno externo e interno, así como los parámetros que deben tenerse en cuenta en la gestión de riesgo, y establece el ámbito de aplicación y criterios de riesgo para el proceso restante. Si bien muchos de estos parámetros son similares a los considerados en el diseño de los riesgos.

Marco de gestión (ver 4.3.1. de la norma ISO 31000), al establecer el contexto para el proceso de gestión del riesgo, es necesario considerar en mayor detalle y en particular cómo se relacionan con el ámbito de los riesgos individuales con el proceso de gestión.

Establecer el contexto externo

El contexto externo es el entorno externo en el que la organización busca alcanzar sus objetivos.

Comprender el contexto externo es importante para garantizar que los objetivos y las preocupaciones de los externos interesados en la compañía se consideran en el desarrollo de los criterios de riesgo. Se basa en el contexto organizacional más amplio, pero con detalles específicos de los requisitos legales y reglamentarios,

CAPITULO II Marco Conceptual, Teórico y Legal

las percepciones de los interesados y otros aspectos de los riesgos específicos para el ámbito de aplicación del proceso de gestión de riesgos.

Establecer el contexto interno

El contexto interno es el ambiente interno en el que la organización busca alcanzar sus objetivos.

El proceso de gestión de riesgos debe estar alineado con la cultura de la organización, procesos, estructura y estrategia. El contexto interno es cualquier cosa dentro de la organización que puede influir en la manera en la que una organización va a gestionar el riesgo. Debe establecerse debido a que:

- a) La gestión del riesgo tiene lugar en el contexto de los objetivos de la organización;
- b) Los objetivos y criterios de un determinado proyecto, proceso o actividad debe ser considerada a la luz de objetivos de la organización en su conjunto, y
- c) algunas organizaciones no reconocen las oportunidades para alcanzar sus objetivos estratégicos, de proyectos o de negocios, y esto afecta en marcha el compromiso organizacional, credibilidad, confianza y valor.

Establecer el contexto del proceso de gestión de riesgos

Los objetivos, estrategias, alcance y los parámetros de las actividades de la organización, o las partes de la organización en el proceso de gestión de riesgo que se están aplicando, deben ser establecidos. La gestión de riesgo debe llevarse a cabo con plena consideración de la necesidad de justificar los recursos utilizados en la realización de gestión de riesgos. Los recursos necesarios, las responsabilidades y autoridades, así como los registros que deben mantenerse también deben ser especificados.

El contexto del proceso de gestión del riesgo puede variar de acuerdo a las necesidades de una organización.

Definición de criterios de riesgo

La organización debe definir los criterios que se utilizarán para evaluar la importancia del riesgo. Los criterios deben reflejar los valores de la organización, objetivos y recursos. Algunos criterios pueden ser impuestos o derivar de requisitos legales o reglamentarios y otros requisitos que la organización suscriba. Los criterios de riesgo deben ser coherentes con la política de gestión de la organización de riesgo (ver 4.3.2 de la norma ISO 31000), se definió al principio que cualquier proceso de gestión del riesgo debe revisarse continuamente.

La definir los criterios de riesgo, factores a considerar deben incluir los siguientes:

- La naturaleza y los tipo de causas y consecuencias que pueden ocurrir y como se mide;
- Como la probabilidad será definido;
- El plazo (s) de la probabilidad y/o consecuencia(s);
- Las opiniones de los interesados;
- El nivel en que se convierte en riesgo aceptable o tolerable, y
- Si las combinaciones de los múltiples riesgos que deben tenerse en cuenta y, en caso afirmativo, cómo y qué combinaciones deben ser consideradas.

iii. Evaluación del riesgo: (5.4)

Evaluación de riesgos es el proceso general de identificación de riesgos, análisis de riesgos y evaluación de riesgos.

NOTA ISO / IEC 31010 proporciona orientación sobre las técnicas de evaluación de riesgos

Identificación de riesgos (5.4.2)

La organización debe identificar las fuentes de riesgo, zonas de impactos, los acontecimientos (incluyendo los cambios en las circunstancias) y sus causas y sus posibles consecuencias. El objetivo de este paso es generar una lista completa de los riesgos basados en los acontecimientos que puedan crear, mejorar, prevenir, degradar, acelerar o retrasar la consecución de los objetivos. Es importante identificar los riesgos asociados a la pérdida de una oportunidad. La identificación completa es fundamental, porque el riesgo de que no se identifique en esta etapa no se incluye en el análisis posterior.

La identificación debe incluir los riesgos si su fuente se encuentra bajo el control de la organización o no, incluso aunque la fuente de riesgo o causa no pueda ser evidente. La identificación de riesgos debe incluir el examen de los efectos encadena de consecuencias particulares, incluidos los de cascada y los efectos acumulativos.

Así como la identificación de los que podría suceder, es necesario considerar las posibles causas y situaciones que muestran que consecuencias pueden ocurrir. Todas las causas y consecuencias importantes deben ser consideradas.

La organización debe aplicar herramientas de identificación de riesgos y técnicas que se adaptan a sus objetivos y capacidades, y de los riesgos que enfrentan. Esto debe incluir información de antecedentes de la manera más adecuada que sea posible. Las personas con los conocimientos adecuados deberían de participar en la identificación de riesgos.

El análisis de riesgos

El análisis de riesgos implica el desarrollo de la comprensión de los riesgos. El análisis de riesgos proporciona una entrada de los riesgos a la evaluación y las decisiones sobre si los riesgos necesitan ser tratados, y el tratamiento del riesgo más adecuado así como la estrategia y métodos.

El análisis de riesgos implica la consideración de las causas y las fuentes de riesgo, sus consecuencias positivas y negativas y la probabilidad de que esas consecuencias pueden ocurrir. Los factores que afectan a las consecuencias y los riesgos deben ser identificados.

El riesgo es analizado mediante la determinación de las consecuencias y la probabilidad, y otros los atributos de los riesgos. Un evento puede tener múltiples consecuencias y puede afectar a múltiples objetivos. Los controles existentes y su eficacia y eficiencia también deben tenerse en cuenta.

La forma en que las consecuencias y la probabilidad se expresan y la forma en que se combinan para determinar un nivel de riesgo debe reflejar el tipo de riesgo, la información disponible y de la finalidad para la que la salida de la evaluación de riesgos se va a utilizar. Todo ello debe ser coherente con los criterios de riesgo. También es importante considerar la independencia de los diferentes riesgos y sus fuentes.

La confianza en la determinación del nivel de riesgo y su sensibilidad a las condiciones previas y las hipótesis debe ser considerada en el análisis, y comunicarse eficazmente a los tomadores de decisiones y en su caso a las partes interesadas.

El análisis de riesgos puede llevarse a cabo con diferentes grados de detalle, dependiendo del riesgo, como el objetivo del análisis, la información, datos y los recursos disponibles. El análisis pueden ser cualitativos, cuantitativos o semi – cuantitativos, o una combinación de estos, dependiendo de las circunstancias.

Las consecuencias y la probabilidad puede ser determinada por la modificación de los resultados de un evento o serie de eventos, o por extrapolación de los estudios experimentales o de los datos disponibles. Las consecuencias pueden ser expresadas en términos de efectos tangibles.

Evaluación de riesgos.

El propósito de la evaluación de riesgos es ayudar en la toma de decisiones, basada en los resultados de análisis de riesgos, sobre riesgos que necesitan tratamiento y la prioridad para la aplicación del tratamiento.

La evaluación de los riesgos supone la comparación del nivel de riesgo identificado durante el proceso de análisis con criterios de riesgo establecidos cuando se considera el contexto. Basándose en esta comparación, se determina la necesidad de que el tratamiento puede ser considerado.

Las decisiones deben tener en cuenta el contexto más amplio del riesgo y de incluir la consideración de la tolerancia de los riesgos asumidos por otras partes de la organización que se beneficia de los riesgos. Las decisiones deben tomarse en conformidad con los requisitos legales, reglamentarios y otros.

En algunas circunstancias, la evaluación del riesgo puede llevar a una decisión de proceder a su posterior análisis. La evaluación de riesgos también puede dar lugar o no a una decisión de tratar el riesgo de cualquier otra forma o de mantener los controles existentes. Esta decisión se verá influida por la actitud ante el riesgo de la organización y los criterios de riesgo.

iv. Tratamiento del riesgo: (5.5)

El tratamiento del riesgo consiste en seleccionar una o más opciones de modificación de los riesgos y la aplicación de esas opciones.

Una vez en marcha, los tratamientos de proporcionar o modificar los controles.

El tratamiento del riesgo implica un proceso cíclico de:

CAPITULO II Marco Conceptual, Teórico y Legal

- La evaluación de un tratamiento del riesgo;
- Decidir si los niveles de riesgo residual son tolerables;
- Si no son tolerables, generando un nuevo tratamiento del riesgo;
- La evaluación de la eficacia de ese tratamiento.

Las opciones de tratamiento de los riesgos no son necesariamente excluyentes o apropiadas en todas las circunstancias. Las opciones pueden incluir los siguientes:

- a) Evitar el riesgo al decidir no iniciar o continuar con la actividad que da lugar al riesgo;
- b) Tomar o aumentar el riesgo con el fin de perseguir una oportunidad;
- c) Eliminar la fuente de riesgo;
- d) Los cambios en la probabilidad;
- e) Cambiar las consecuencias;
- f) La distribución del riesgo con otra parte o partes (incluidos los contratos y la financiación de riesgo), y
- g) Mantener el riesgo por decisión informada.

Selección de opciones de tratamiento del riesgo

Selección de la opción de tratamiento más adecuado de riesgos consiste en equilibrar los costes y los esfuerzos de la aplicación contra los beneficios obtenidos, con respecto a los requisitos legales, reglamentarios y otros, tales como la responsabilidad social y la protección del medio ambiente natural.

Preparación y ejecución de planes de tratamiento del riesgo

El objetivo de los planes de tratamiento del riesgo es documentar cómo las opciones de tratamiento elegidos se llevarán a cabo.

La información proporcionada en los planes de tratamiento debe incluir:

CAPITULO II Marco Conceptual, Teórico y Legal

- Las razones para la selección de opciones de tratamiento, incluyendo los beneficios esperados que se pueden obtener;
- Los que son responsable de aprobar el plan y los responsables de la ejecución del plan;
- Acciones propuestas:

Las necesidades de recursos – incluidas las contingencias;

- Medidas de rendimiento y limitaciones;
- Presentación de informes y los requisitos de control, y
- Calendarios y horarios.

Los planes de tratamiento deben ser integrados con los procesos de gestión de la organización y discutido con las partes interesadas pertinentes.

Los tomadores de decisiones y otras partes interesadas deben ser conscientes de la naturaleza y el alcance de riesgo residual después del tratamiento del riesgo. El riesgo residual debe ser documentado y sometidos a la supervisión y, cuando su caso, el tratamiento adicional.

e) Aplicación y Beneficios de la Norma ISO 31000

En resumen, el estándar ISO 31000 adopta lo mejor del mundo gerencial y de riesgos, a diferencia de otras ISO, la ISO 31000:2009, no exige certificación, pero pretende que la norma sea utilizada para armonizar los procesos de gestión de riesgos con las normas existentes y futuras. Además, proporciona un enfoque común en favor de otras normativas que tratan sobre riesgos específicos y / o sectores, y no las sustituyen.

Finalmente, en cuanto a los beneficios, éstos se relacionan principalmente a:

- Aumentar la probabilidad de lograr los objetivos;
- Fomentar una gestión proactiva;
- Ser consciente de la necesidad de identificar y tratar los riesgos en toda la organización;

CAPITULO II Marco Conceptual, Teórico y Legal

- Mejorar la identificación de las oportunidades y amenazas;
- Cumplir con las exigencias legales y reglamentarias y las normas internacionales;
- Mejorar la información financiera;
- Mejorar la gobernabilidad;
- Mejorar la confianza de los grupos de interés (stakeholder);
- Establecer una base confiable para la toma de decisiones y la planificación;
- Mejorar los controles;
- Efectivamente asignar y utilizar recursos para el tratamiento del riesgo;
- Mejorar la eficacia y eficiencia operativa;
- Mejorar la salud y de seguridad, así como la protección del medio ambiente;
- Mejorar la prevención de pérdidas y de manejo de incidentes;
- Reduzca al mínimo las pérdidas;
- Mejorar el aprendizaje organizacional; y
- Mejorar la capacidad de recuperación de la organización.

Lo importante en la adopción de un modelo de gestión de riesgos es que este sea fácilmente comprensible en la organización, que sea el directorio quien tome decisiones basadas en riesgos, que la implementación del modelo sea liderada por la alta gerencia y finalmente que la responsabilidad de los riesgos sea encabezada por unidades de negocio y sus áreas funcionales, para lograr un manejo inteligente en materia de riesgos.

7. MARCO TEÓRICO Y LEGAL

De acuerdo con la normativa legal y teórica en el Sector Público Boliviano, con referencia en la administración del riesgo operativo aplicable al Sector Público Financiero no Bancario, y solo existe una aproximación a lo que es Gestión de Riesgos con la implementación del Sistema de Control Gubernamental determinado en la Ley 1178 LEY DE ADMINISTRACIÓN Y CONTROL GUBERNAMENTALES (Ley

SAFCO), sistema que consiste la aplicación del modelo de control interno para la evaluación de riesgos en el sector público.

En el ámbito privado la Ex Superintendencia de Bancos y Entidades Financieras - SBEF y actualmente Autoridad de Supervisión del Sistema Financiero - ASFI ha emitido Guías para la Gestión de Riesgos, que se enmarca en base a los Principios y Pilares de Basilea II con referencia al riesgo, el documento está estructurado definiendo la Gestión Integral de Riesgos para su aplicación en entidades de intermediación financiera, define las políticas y la Gestión de los Riesgos de Crédito, Mercado, Tasas de Interés, Tipo de Cambio, Liquidez y Operativo.

A continuación se analiza y revisa los documentos relacionados con el marco teórico y legal sobre la gestión de riesgos en Bolivia:

1.1 Principios, Normas Generales y Básicas de Control Gubernamental

Este documento ha sido aprobado el 21/09/2000 por la Ex Contraloría General de la República actualmente Contraloría General del Estado, este documento fue emitido por el órgano rector del sistema de control gubernamental en base a la Ley N° 1178, del 20 de Julio de 1990, procurando dotar al Estado Boliviano de sistemas modernos de gestión pública, cuya implantación se inició con la emisión y la aplicación de normas generales y básicas de control interno para cada sistema de administración emitidas, en primera instancia, en septiembre de 1992 por la Contraloría General de la República (CGR), las que fueron revisadas y reemplazadas en noviembre de 1996. Posteriormente, el Ex Ministerio de Hacienda actualmente Ministerio de Economía y Finanzas Públicas (Organo Rector de los Sistemas de Administración) procedió a la emisión de Normas Básicas para cada uno de ellos en la gestión 1993 completándose el proceso con modificaciones en la gestión 2005.

Debido al tiempo transcurrido las referidas Normas Básicas de Control Interno, estas fueron revisadas y actualizadas, en atención a las necesidades y dinámicas relacionadas con los siguientes conceptos:

CAPITULO II Marco Conceptual, Teórico y Legal

- Evaluación del ambiente y de las actividades de control para la minimización de los riesgos y jerarquización de controles, en el cumplimiento de los objetivos de las entidades del sector público (Informe COSO)
- Administración por objetivos y evaluación de resultados
- Responsabilidad
- Compromiso social en el marco del desarrollo sostenible
- Aseguramiento de la calidad
- • Desarrollo científico y tecnológico.

Como puede observarse el alcance de las modificaciones de los principios y normas de control interno de Gubernamental fueron realizados en base al informe COSO I explicado detalladamente en el punto 10 de este proyecto.

1.2 Marco Legal del Sistema de Control Interno Gubernamental Boliviano

La Ley N° 1178 en su Art. 13° establece que el Control Gubernamental estará integrado por el Sistema de Control Interno, compuesto por instrumentos de control previo y posterior y el Sistema de Control Externo Posterior.

El Art. 23° de la referida Ley establece que la Contraloría General de la República es el órgano rector del Sistema de Control Gubernamental, el cual se implantará bajo su dirección y supervisión; emitirá las normas básicas de control interno y externo; evaluará la eficacia de los sistemas de control interno; realizará o supervisará el control externo realizado por firmas o profesionales calificados e independientes, contratados a esos fines.

El Art. 3° del Reglamento aprobado por el D.S. N° 23215, detalla las atribuciones conferidas a la Contraloría General de la República por la Ley N° 1178, entre ellas la atribución de elaborar y emitir la normatividad básica de Control Gubernamental Interno y Posterior Externo.

En concordancia con lo anterior, el Art. 18° del citado Reglamento determina que las Normas Básicas de Control Gubernamental Interno son emitidas por la Contraloría

General de la República, forman parte integral del control gubernamental y son normas generales de carácter principista que definen el nivel mínimo de calidad para desarrollar adecuadamente las políticas, los programas, la organización, la administración y el control de las operaciones de las entidades públicas. Establece, además, que estas normas deben ser tenidas en cuenta por el órgano rector de los Sistemas de Administración en el diseño y desarrollo (implantación, evaluación y actualización) de los mismos y por las entidades públicas en la elaboración de la normatividad secundaria, esto es, los reglamentos, manuales, instructivos o guías emitidos por los ejecutivos y aplicados por las propias entidades.

a) **Conceptualización del control interno**

En el documento de los Principios, Normas Generales y Básicas de Control Interno Gubernamental en base al modelo COSO I se define el control interno:

*“El Control Interno es **un proceso** compuesto por una cadena de acciones extendida a todas las actividades inherentes a la gestión, **integradas a los procesos** básicos de la misma e incorporadas a la infraestructura de la organización, bajo la responsabilidad de su consejo de administración y su máximo ejecutivo, llevado a cabo por éstos y por todo el personal de la misma, **diseñado con el objeto de limitar los riesgos internos y externos** que afectan las actividades de la organización, **proporcionando un grado de seguridad razonable** en el cumplimiento de los objetivos de eficacia y eficiencia de las operaciones, de confiabilidad de la información financiera y de cumplimiento de las leyes, reglamentos y políticas, así como las iniciativas de calidad establecidas ”.*

La visión brindada por esta definición es la adoptada como sustento de los Principios y Normas Generales y Básicas de Control Interno Gubernamental, en total coincidencia con lo establecido en materia de control gubernamental por la Ley N° 1178.

b) Estructura de los Principios, Normas Generales y Básicas de Control Interno

La organización y estructura de esta norma boliviana de control interno responde a criterios fundamentados en diferenciar la naturaleza del control interno de las entidades públicas y de sus recursos humanos, con la orientación hacia el logro de objetivos institucionales concordantes con la estrategia, en un marco de calidad, contemplando los postulados de la Ley N° 1178.

Desde este punto de vista, la naturaleza del control interno radica en el diseño e implantación de actividades, que aseguren la minimización de los riesgos en el cumplimiento de los objetivos institucionales, en un ambiente de control adecuado, contemplando una jerarquía acorde con la establecida para la estructura organizativa. Este proceso de control debe ser desarrollado y ejecutado, por personal en pleno ejercicio del criterio y juicio profesional, respetando el concepto básico de responsabilidad y para el aseguramiento y mejoramiento continuo de la calidad.

Del enfoque precitado, resultan los siguientes principios, entendidos como razón o idea fundamental, consensuada y aceptada profesionalmente, para orientar la concepción del proceso de control interno:

- Naturaleza de control interno
- Calidad de control interno
- Responsabilidad
- Jerarquía de los controles
- Criterio y juicio personal y profesional

Los principios señalados, fueron los parámetros básicos que orientaron a la Contraloría General de la República para formular las normas generales.

Las normas generales, se han desarrollado según los componentes del proceso de control interno, definidos en el informe COSO I y contemplando la gestión de la calidad, en consecuencia se refieren al:

- Ambiente de control
- Evaluación de riesgos
- Actividades de control
- Información y comunicación
- Supervisión
- Calidad

Las referidas normas deben entenderse como reglas que, sobre la base de los principios y con una vigencia temporal, establecen los aspectos a los que se debe ajustar el proceso de control interno el cual forma parte integrante del control gubernamental.

En cuanto a las normas básicas, tienen como fin, como reglas derivadas de cada una de las normas generales, contribuir al mejor entendimiento de estas últimas y posibilitar el diseño, implantación y funcionamiento del proceso de control interno en las organizaciones públicas.

1.3 **Guía para la aplicación de los principios, normas Generales y Básicas de Control Interno Gubernamental CI/10**

Este documento de apoyo para la implantación de los Principios, Normas Generales y Básicas de Control Interno Gubernamental CI/08, fue aprobado el 31/10/2002 con resolución CGR-1/173/2002 y entra en vigencia a partir del 1/12/2002 para que sean consideradas por todas las entidades públicas en todas sus partes, en la normatividad secundaria que se emitirá.

a) Estructura de la Guía CI/10

Este documento base para la aplicación de los Principios, Normas Generales y Básicas de Control Interno Gubernamental, está estructurado de manera didáctica para su utilización y comprende los siguientes temas:

- Conceptualización del Control Interno

- Diseño y estrategia para la implantación del Control Interno
- Desarrollo de los Componentes de Control Interno en base al COSO I

Sin embargo, de acuerdo al objeto de este proyecto se analizará el componente Evaluación de Riesgos.

b) Evaluación de Riesgos según CI/10

La Guía CI/10, estructura un procedimiento de evaluación de riesgos así como métodos, herramientas para la implantación de este componente de control interno.

Determina el objetivo de la evaluación de riesgos, los insumos del proceso de evaluación de riesgos, la instrumentación de los sistemas de alerta tempranos, los riesgos que se deben identificar, métodos para la identificación de riesgos, objetivos y riesgos relacionados con los sistemas operativos y administrativos, método para el análisis de riesgos (Mapa de riesgos) y el manejo de riesgos en función al nivel de riesgo establecido.

Ya en este documento se describe la necesidad de un sistema de gestión de riesgos, porque la evaluación de riesgos concluye con el análisis de los mismos. Los resultados de dicho análisis deberán ser utilizados por la dirección de la entidad para establecer la mejor forma de gestionarlos.

En cambio la Gestión de Riesgos implica la determinación, implantación, políticas programas y acciones que los sectores administrativos y operativos deben llevar a cabo.

La gestión de riesgos actúa como un nexo entre la evaluación de riesgos y las actividades de control, se constituye una actividad neta de gestión y no forma parte del proceso de control interno.

c) Concepto de Riesgos según CI/10

Se conceptualiza el riesgo como *la posibilidad de ocurrencia de cualquier situación que afecte el desarrollo de las operaciones y puede perjudicar el logro de objetivos de la entidad*. En general, el riesgo implica la posibilidad de una pérdida económica. Dicha pérdida puede estar presentada por mayores costos operativos, menor calidad de los productos o servicios, o retrasos en la ejecución de los procesos.

En general el éxito de una entidad depende del cumplimiento de los objetivos y éste se condicionado por una efectiva gestión o administración de riesgos que pueda limitar la posibilidad de ocurrencia de pérdidas de cualquiera naturaleza.

1.4 Guía para la implantación del Control Interno G/CE-21

Este documento de carácter normativo secundario de control para la implantación del Control Interno Gubernamental G/CE -21, fue aprobado el 23/10/2008 con resolución CGR-1/245/2008, y por ser norma secundaria de los Principios, Normas Generales y Básicas de Control Interno (CI/08) Versión 3, es de aplicación obligatoria para todas las entidades públicas en la implantación del proceso de control Interno.

a) Objetivo y estructura de la Guía G/CE-21

La Guía tiene como objeto fundamental el establecimiento del control interno en las entidades del sector público bajo características de practicidad, considerando los ajustes pertinentes de acuerdo con su naturaleza, tamaño, complejidad y niveles de implantación de sus controles internos.

El proceso de implantación del control interno genera la necesidad de un diseño o rediseño organizacional, el mismo que debe ser formalizado a través del Manual de Organización y Funciones, Manual de Procesos y, de los reglamentos específicos de los Sistemas de Administración establecidos en la Ley N° 1178; documentos que deben ser compatibilizados cuando corresponda y aprobados por autoridad pertinente.

Este documento normativo define el concepto de riesgo en base al COSO ERM, es decir, *“Riesgo es la posibilidad de que un evento ocurra y afecte adversamente a la consecución de objetivos”*.

Además establece el alcance de este documento, definiciones principales, la metodología para la implantación del control interno, la estructura del control interno y el desarrollo de objetivos, criterios y acciones para cada componente de control interno.

Esta guía refleja la interrelación entre objetivos y componentes de control interno, de tal forma que una relación directa entre objetivos, los cuales son el resultado que una entidad busca conseguir, y los componentes, factores y subcomponentes, coadyuvan a la consecución de objetivos.

b) Evaluación de Riesgos según la Guía G/CE-21

En esta Guía desarrolla el modelo de evaluación de riesgos aplicarse en las entidades públicas, con el enfoque de que el control interno ha sido pensado esencialmente para limitar riesgos que afectan a las operaciones de las organizaciones. A través de la investigación y análisis de los riesgos relevantes, tanto derivados de la situación presente como del efecto de los cambios futuros que deben anticiparse por medio de sistemas de alertas tempranos, se identifica el punto hasta el cual el control vigente los neutraliza y se evalúa la vulnerabilidad del sistema. Para ello, establece que debe adquirirse un conocimiento práctico de la entidad y sus componentes; asimismo, identificar los puntos débiles, riesgos internos y externos que pueden afectar las actividades de la organización.

c) Subcomponentes de la Evaluación de Riesgos según la Guía G/CE-21

Los subcomponentes del componente evaluación de riesgos incluyen la identificación de eventos, evaluación y respuesta a los riesgos.

i. Subcomponente: Identificación de Eventos

Involucra la caracterización de eventos potenciales de fuentes internas o externas que afectan el logro de los objetivos. Incluye la distinción entre eventos que representan riesgos, oportunidades o ambas. Las oportunidades se reenvían hacia la estrategia de la dirección o a los procesos para el logro de los objetivos.

De acuerdo a la metodología de la Guía, se deben establecer los objetivos funcionales, los criterios y las acciones para la identificación de eventos.

Control	Medio
Identificar Eventos	<ul style="list-style-type: none"> - Metodología para la identificación de eventos. - Matriz de Configuración de Eventos.

Como Identificar los Eventos

Para la identificación de eventos la entidad debe contar con una metodología que determine las técnicas y herramientas aplicables que le permita conocer ¿Qué puede suceder? y ¿Cuándo, Dónde y Cómo puede suceder? La aplicación de dicha metodología debe permitir la elaboración de una Matriz de Configuración de Riesgos.

Responsables de elaborar la metodología

La metodología para la identificación de eventos y la Matriz de Configuración de Riesgos debe ser elaborada por la unidad responsable de la Gestión de Riesgos (UGR). Dicha unidad, desarrollar al menos las siguientes funciones:

- Diseñar y actualizar los procesos de gestión de riesgos.
- Coordinar las actividades para la identificación y análisis de riesgos.
- Determinar las características del proceso de respuesta al riesgo incluyendo los planes de contingencia.

CAPITULO II Marco Conceptual, Teórico y Legal

- Centralizar y compatibilizar la información de identificación, análisis y alternativas de tratamiento de los riesgos.
- Preparar los informes de riesgos para el Comité de Gestión de Riesgos y otros interesados (Directorio, Consejos de Administración, etc.).

Principales tareas a desarrollarse

Para elaborar la metodología que permita identificar eventos se deben realizar, al menos, las siguientes tareas:

- Determinar la combinación de técnicas más adecuadas para la entidad.
- Establecer los insumos necesarios para la aplicación de las técnicas seleccionadas.
- Definir los responsables de la aplicación de las técnicas.
- Determinar las tareas para el desarrollo de las técnicas.
- Establecer el momento en que se deben aplicar las técnicas.
- Mencionar el producto a obtener de las técnicas establecidas y su destinatario.

Técnicas aplicables para la identificación de Eventos

Debe definirse la metodología para la identificación de Riesgos a través de las Técnicas para la identificación de eventos, como por ejemplo las siguientes:

- **Workshops:** Esta técnica identifica los eventos utilizando el conocimiento acumulado y experiencia de los ejecutivos y otro personal a través de discusiones estructuradas. El facilitador o entrevistador conduce la discusión sobre los eventos que pueden impactar en el logro de los objetivos de la entidad o unidad. Combinando el conocimiento y experiencia de miembros del equipo se identifican los eventos potenciales que de otra manera podrían ser desconocidos.
- **Inventario de eventos:** Consiste en un detalle de eventos potenciales comunes a las entidades que prestan servicios similares. Por ejemplo:

CAPITULO II Marco Conceptual, Teórico y Legal

entidades relacionadas con los servicios de salud, o educación, o entidades fiscalizadoras. Dichas entidades pueden utilizar listas genéricas como punto de partida para las actividades de identificación de eventos.

- **Análisis interno y externo:** Esta técnica se puede utilizar como parte del proceso de planificación vía reuniones con el personal de las unidades operativas. El análisis interno puede requerir información de terceros (usuarios y proveedores) o especialistas en la materia (expertos externos conocedores de las operaciones de la entidad y personal de auditoría interna). Este análisis se puede materializar en un esquema FODA (Fortalezas, Oportunidades, Debilidades y Amenazas).
- **Definición de márgenes de tolerancia:** Estos márgenes alertan a los ejecutivos sobre las áreas potenciales de preocupación comparando las transacciones actuales, o eventos con criterios predefinidos. Cuando un evento ha llegado al margen, la entidad o unidad correspondiente realizará una nueva evaluación o tomará una acción de respuesta inmediata.
- **Base de datos de eventos:** La base de datos sobre eventos individuales negativos que se han generado en el pasado representan una fuente de información útil para identificar tendencias y las causas principales. Una vez que se ha identificado una causa principal, las unidades pueden determinar cuál es la evaluación y el tratamiento más eficaz que dirigiéndose a los eventos individuales. Este análisis permite identificar las causas principales de los eventos y tomar las acciones necesarias.
- **Análisis del flujo de los procesos:** Esta técnica considera la combinación de entradas, tareas, responsabilidades y rendimientos que se relacionan para formar un proceso. Considerando los factores internos y externos que afectan las entradas, o actividades dentro de un proceso, una entidad identifica eventos que podrían afectar el logro de objetivos de dicho proceso.

Como Producto de este subcomponente se obtiene la Matriz de Configuración de Eventos de acuerdo a la Figura 10, para continuar con la siguiente fase de la Categorización de Eventos.

Factor	Fuente	Evento	Controles	Causas	Consecuencias
A nivel entidad					
Políticos	Decretos	Cambios en las regulaciones	No se han diseñado controles	Presiones sociales	Incumplimiento de leyes
Otros					
A nivel unidad					
Unidad de Presupuesto					
Personal	Directrices Presupuestarias	Errores en la formulación de gastos	Comunicación interna sobre techos presupuestarios	Inexistencia de supervisión	Rechazo del anteproyecto de presupuesto por parte del Ministerio de Hacienda
Otros					

Figura 10 Matriz de Configuración de Eventos

Categorización de Eventos

Uno de los procesos para la implantación de la metodología es el siguiente:

Control	Medio
Categorizar Eventos	Clasificación de eventos a través de una Matriz de Configuración de Eventos.

Categorizar los Eventos

Para categorizar eventos la entidad debe realizar una clasificación a nivel entidad y a nivel de las unidades que la conforman.

La categorización de eventos permite obtener una visión de portafolio (visión general) de los eventos a nivel entidad por objetivo estratégico y objetivo institucional, y a nivel de unidades organizacionales por objetivo de gestión relacionado.

Responsables de la Categorización

La clasificación de eventos debe ser procesada por la unidad responsable de Gestión de Riesgos (UGR) con el apoyo del resto de las unidades, quienes deben elaborar la información de sus objetivos de gestión y los eventos relacionados.

Principales tareas para categorizar

Para clasificar los eventos se deben realizar, al menos, las siguientes tareas:

- Obtener la identificación de eventos.
- Obtener los objetivos a nivel de entidad.
- Obtener los objetivos desagregados a nivel de unidades organizacionales.
- Imputar los eventos que afectan a toda la entidad (clasificación horizontal).
- Imputar los eventos que afectan a cada unidad (clasificación vertical).

La categorización de eventos relacionados con los objetivos de la entidad y de sus unidades organizacionales deben tabularse en una matriz de eventos, los cuales deben ser clasificados, en primer lugar, los eventos previamente identificados deben ser presentados horizontalmente a lo largo de toda la entidad y, posteriormente, se presentan verticalmente los eventos vinculados con cada unidad organizacional y sus objetivos de gestión a esta matriz se la denomina MATRIZ DE EVENTOS – Horizontal y Vertical. Ver Figura 11

UNIDADES OBJETIVOS	UNIDADES OPERATIVAS			UNIDADES ADMINISTRATIVAS			
	A	B	C	1	2	3	4
Objetivos Estratégicos	EVENTOS A NIVEL ENTIDAD (horizontal)						
1-	→						
Objetivos Institucionales	EVENTOS A NIVEL ENTIDAD (horizontal)						
1-	→						
Objetivos de las unidades	EVENTOS A NIVEL UNIDAD (vertical)						
1-	↓						

Figura 11 Matriz de Eventos – Horizontal y Vertical

Relacionamiento de Eventos

El proceso sugerido para implantar este proceso es:

Control	Medio
Relacionar eventos	Matriz de Eventos Interrelacionados para el análisis de relación.

Categorizar los Eventos

Para relacionar los eventos la entidad debe realizar un análisis de relación que se exterioriza en la Matriz de Eventos Interrelacionados. En este sentido, se debe considerar que los eventos no siempre ocurren en forma independiente. Un evento puede desencadenar otros eventos. Por ejemplo: Algunos eventos externos como la modificación en los tipos de cambio generados por la autoridad monetaria del país puede generar eventos relacionados con la exactitud de las operaciones de la unidad de contabilidad. Asimismo, eventos internos relacionados con algunas unidades operativas o administrativas pueden desencadenar eventos en otras unidades. Por ejemplo: el mantenimiento inadecuado de los programas por la unidad de sistemas puede generar eventos de información errónea en las unidades operativas.

Responsables de la Categorización

La Matriz de Eventos Interrelacionados debe ser elaborada por la unidad responsable de Gestión de Riesgos con el apoyo del resto de las unidades que deben elaborar la identificación de sus eventos.

Principales tareas para categorizar

Para relacionar los eventos se deben realizar, al menos, las siguientes tareas:

- Obtener la Matriz de Eventos identificados.
- Obtener los Eventos de las Operaciones.

CAPITULO II Marco Conceptual, Teórico y Legal

- Determinar el posible encadenamiento de algunos eventos de la entidad con los eventos de las unidades organizacionales.
- Determinar el posible encadenamiento de algunos eventos de las unidades respecto de las unidades de apoyo (administrativas) u otras unidades operativas.
- Elaborar una matriz de encadenamiento para poder centralizar los esfuerzos de la administración de riesgos.

En la Figura 12, se presenta la matriz de eventos interrelacionados, que muestra la relación de los eventos entre una Unidad “afectada”, la Unidad organizacional y los eventos de la Entidad.

Eventos a Nivel de Entidad		Unidad Afectada	Eventos relacionados
1.-		Unidad SABS	1.-
2.-		Unidad SAP	1.-
Eventos a Nivel de Unidad Organizacional			
Unidad Organizacional	Eventos		
Unidad SP	1.-	Unidad SABS	1.-
Unidad SAP	1.-	Unidad Operativa A	1.-

Figura 12 Matriz de Eventos interrelacionados

ii. Subcomponente: Evaluación de Riesgos

Los riesgos identificados son evaluados para establecer una base y determinar cómo deben ser administrados, se asocian con los objetivos que pueden afectar y son evaluados sobre una doble perspectiva inherente y residual, considerando su probabilidad e impacto.

De acuerdo a la metodología de la Guía, se deben establecer los objetivos funcionales, los criterios y las acciones para la valoración los Riesgos.

Determinación de la Consecuencia y Probabilidades

Control	Medio
Establecer criterios de valoración	Escala de valores para consecuencias y probabilidades

Establecer los Criterios de Valoración

Para establecer los criterios de valoración de riesgos la entidad debe contar con escalas de valores determinados por importancia relativa de las consecuencias, frecuencia de ocurrencia y probabilidades.

Las escalas habitualmente tienen un mínimo de tres niveles aunque existen escalas más complejas de cuatro, cinco y seis niveles para considerar el impacto de los eventos y su probabilidad de ocurrencia.

Responsables de la Elaboración de Criterios

Las escalas de valores de las consecuencias y probabilidades deben ser elaboradas por la unidad responsable de Gestión de Riesgos.

Tareas para la evaluación de Riesgos

Para elaborar las escalas se deben realizar, al menos, las siguientes tareas:

- Establecer los niveles junto a la definición y descripción de cada uno de ellos para los impactos o consecuencias de los eventos.
- Establecer los niveles junto a la definición y descripción de cada uno de ellos para las probabilidades de ocurrencia de los eventos.
- Definir el horizonte del tiempo al cual se refiere la escala de probabilidades de ocurrencia y los criterios aplicables.
- Definir los criterios a considerar para establecer los niveles de las magnitudes de los eventos.

CAPITULO II Marco Conceptual, Teórico y Legal

Con relación al horizonte de tiempo para definir si un evento ocurre o podría ocurrir con mayor o menor frecuencia o probabilidad, se debe considerar 1 año a efectos de la identificación de eventos relacionados con los objetivos institucionales y de gestión de las unidades organizacionales. Para los eventos relacionados con los objetivos estratégicos se debe tomar en cuenta la duración del período estratégico.

Respecto de la identificación de eventos a nivel de procesos y procedimientos, es conveniente considerar los siguientes criterios:

- La cantidad de veces que el procedimiento se desarrolla dentro de una gestión y si el evento puede ocurrir en todos los procedimientos, o en algunos; y
- La cantidad de veces que el evento ocurre en cada procedimiento; siendo factible que ocurra una vez o en varias oportunidades; o nunca.

A manera de ejemplo se presentan en la Figura 13 las siguientes escalas aplicables para la frecuencia de ocurrencia:

Nivel	Definición	Descripción
1	Remoto	El evento es infrecuente o se presume que no podría ocurrir.
2	Posible	El evento ocurre frecuentemente o se presume que posiblemente ocurrirá.
3	Probable	El evento ocurre muy frecuentemente o se presume que seguramente ocurrirá.

Figura 13 Frecuencia de Ocurrencias (FO)

En cuanto a la importancia relativa se deben considerar, al menos, los siguientes criterios:

Objetivos relacionados con el cumplimiento de leyes y normas:

- Consecuencias penales y su relación con los intereses del estado y la sociedad.

CAPITULO II Marco Conceptual, Teórico y Legal

- Consecuencias civiles y su relación con los intereses del estado y la sociedad.
- Consecuencias administrativas y su relación con los intereses del estado y la sociedad.

Asimismo, se deben considerar los intereses del directorio cuando corresponda y la máxima autoridad ejecutiva respecto del cumplimiento de leyes y normas independientemente de los posibles montos relacionados con los eventos.

Objetivos relacionados con la confiabilidad de la información financiera:

- – Valor estimado de la consecuencia sobre el valor de los activos totales.
- – Valor estimado de la consecuencia sobre el valor del patrimonio.
- – Valor estimado de la consecuencia sobre el valor de los ingresos.
- – Valor estimado de la consecuencia sobre el valor de los gastos.

Objetivos relacionados con la eficacia y eficiencia operativa:

- Consecuencia sobre el objetivo del proceso o procedimiento.
- Consecuencia sobre el objetivo de gestión del área o unidad organizacional.
- Consecuencia sobre el objetivo estratégico relacionado.
- Consecuencia sobre el valor de los activos o bienes de uso al cierre de un período determinado.
- Consecuencia sobre el valor del dinero disponible en un período determinado.

Asimismo, se deben considerar los perjuicios que se pueden generar en la imagen de la institución y las prioridades que hayan establecidos los ejecutivos en relación con la eficacia y eficiencia de las operaciones independientemente de los posibles montos relacionados.

No obstante, para los objetivos operacionales es indispensable que la entidad haya definido la “Tolerancia al Riesgo” que constituye el desvío aceptable en el

logro de los objetivos. La tolerancia al riesgo representa el marco dentro del cual se valorarán las consecuencias de los eventos operacionales.

A manera de ejemplo en la Figura 14 se presentan las siguientes escalas aplicables para determinar el nivel de Importancia Relativa:

Nivel	Definición	Descripción
1	Poco significativo	La consecuencia del evento no afectará el logro del objetivo relacionado.
2	Significativo	La consecuencia del evento afectará pero no impedirá el logro del objetivo relacionado.
3	Muy significativo	La consecuencia del evento impedirá el logro del objetivo relacionado.

Figura 14 Importancia Relativa (IR)

Determinación del Nivel de Riesgo

Control	Medio
Calificar la importancia relativa y frecuencia de ocurrencia para determinar el nivel de riesgos.	Metodología para determinar el nivel de riesgos.

Valoración o Determinación de Riesgos

Para valorar el impacto y la probabilidad de los eventos que mide el nivel de riesgos la entidad debe elaborar una metodología que permita determinar el nivel de riesgos a efectos de enfocar los esfuerzos de tratamiento o respuesta.

Responsables de la Determinación de Riesgos

La metodología para determinar el nivel de riesgos debe ser elaborada por la unidad responsable de Gestión de Riesgos.

No obstante, la valoración debe ser efectuada por los responsables de las áreas y unidades organizacionales que han identificado sus eventos aplicando los criterios preestablecidos y utilizando las escalas disponibles.

Las áreas y unidades deben respaldar sus valoraciones sobre consecuencias y probabilidades para las revisiones que considere necesaria el Comité de Gestión de Riesgos y la unidad encargada de la Gestión de Riesgos.

Tareas para la evaluación de Riesgos

Para establecer la metodología a efectos de determinar el nivel de riesgos se deben realizar, al menos, las siguientes tareas:

- Obtener la lista de eventos identificados a nivel entidad y a nivel de las unidades organizacionales.
- Interpretar las consecuencias y probabilidades de acuerdo con los criterios preestablecidos en la Matriz de Eventos de Riesgos
- Valorar numéricamente las consecuencias y las probabilidades según las escalas preestablecidas en la Matriz de Eventos de Riesgos

En la Figura 15 la matriz de nivel de riesgo se muestra el resultado de la interrelación de las variables de Frecuencia de Ocurrencia (FO) e Importancia Relativa (IR) con las escalas propuestas como ejemplo.

IMPORTANCIA RELATIVA (IR)	FRECUENCIA DE OCURRENCIA (FO)		
	1	2	3
1	Muy Bajo	Bajo	Medio
2	Bajo	Medio	Alto
3	Medio	Alto	Muy Alto

Figura 15 Matriz de Nivel de Riesgos

Determinación del Nivel de Riesgo

Control	Medio
Valoración de eventos correlacionados	Matriz para la Valoración de Eventos Correlacionados.

Valoración de los eventos correlacionados

Para la valoración eventos correlacionados la entidad debe realizar un análisis que se exterioriza en una Matriz para la Valoración de Eventos Correlacionados. Dicha correlación es importante para la valoración de probabilidades e impactos de los eventos. Un evento individualmente considerado puede tener un impacto relativamente bajo, y si el mismo forma parte de una sucesión de varios eventos puede tener un impacto podría ser significativo.

Responsables de la correlación de eventos

El análisis de relación debe ser elaborado por la unidad responsable de Gestión de Riesgos (UGR) con el apoyo de las unidades que presentan eventos correlacionados.

Tareas para la evaluación de Riesgos

Para el análisis de correlación de eventos a efectos de la valoración y elaborar la matriz correspondiente se deben realizar, al menos, las siguientes tareas:

- Obtener la Matriz de Eventos Interrelacionados.
- Reunir a los responsables de las unidades relacionadas.
- Analizar en forma conjunta con los responsables de las unidades vinculadas como varía el impacto o la probabilidad de eventos cuando éstos se correlacionan.
- Retroalimentar la valoración de los eventos individuales que se haya realizado en cada una de las áreas o unidades organizacionales.

A continuación en la Figura 16 se muestra la matriz de eventos correlacionados con la valoración de los eventos en función a la determinación del nivel de riesgo.

EVENTOS CORRELACIONADOS				VALORACIÓN
Eventos a nivel Unidad	Eventos a nivel Unidad	Eventos a nivel Unidad	Eventos a nivel Entidad	
Unidad SABS	Unidad de Sistemas	Unidad Operativa A		
Retrasos en la contratación de programadores de sistemas.	Retrasos en el desarrollo de programas de computación.	Prestación de servicios con errores.	Ineficiencias en el Objetivo XX.	
BAJO	BAJO	ALTO	ALTO	Preliminar
ALTO	ALTO	ALTO	ALTO	Modificado por correlación

Figura 16 Matriz para la Valoración de Eventos Correlacionados

iii. Subcomponente: Respuesta a los Riesgos

Evaluados los riesgos relevantes, la dirección superior determina como responder a ellos, pudiendo. Las respuestas pueden ser las de evitar, aceptar, reducir y compartir. La dirección superior selecciona un conjunto de acciones para poner en línea los riesgos con sus tolerancias respectivas y el riesgo aceptado por la entidad.

De acuerdo a la metodología de la Guía, se deben establecer los objetivos funcionales, los criterios y las acciones para la respuesta a los Riesgos.

Sin embargo los siguientes criterios son importantes a la hora de determinar las acciones

– **Instrumento organizacional:**

La entidad ha elaborado una metodología para evaluar las posibles respuestas al riesgo procurando que el riesgo residual esté alineado con la tolerancia al riesgo.

– **Costo-Beneficio:**

Las respuestas al riesgo deben considerar costos y beneficios directos e indirectos.

El análisis de costo-beneficio permite comparar diferentes respuestas para el tratamiento de un riesgo.

– **Mapa de Riesgos:**

La entidad ha elaborado un mapa de riesgos como parte de su plan de tratamiento de los riesgos para determinar las posibles respuestas que se pueden implementar a partir de las decisiones de la máxima autoridad ejecutiva.

Identificar Respuestas

Control	Medio
Identificar respuestas	Matriz de Respuesta al Riesgo

Identificación de las Respuestas

Para identificar las alternativas existentes para los riesgos evaluados, la entidad debe aplicar la Matriz de Respuesta al Riesgo presentada en la Figura 17.

Se debe considerar que las opciones de respuesta no son mutuamente excluyentes y su aplicación depende de las circunstancias.

Responsables de la correlación de eventos

La Matriz de Respuesta al Riesgo debe ser elaborada por la unidad responsable de Gestión de Riesgos. Dicha Matriz debe ser aprobada por el Comité de Gestión de Riesgos de la entidad.

Tareas para la evaluación de Riesgos

Para elaborar la Matriz de Respuesta al Riesgo se deben realizar, al menos, las siguientes tareas:

- – Establecer y describir las posibles respuestas al riesgo.
- – Determinar el alcance de las posibles respuestas al riesgo.
- – Definir la relación entre nivel de riesgo y respuesta al riesgo.

A continuación se presentan las respuestas al riesgo aplicables y sus características principales:

– Evitar el riesgo

Supone salir de las actividades que generen riesgos. Evitar el riesgo puede implicar el cese de actividades o los bienes riesgosos. No siempre es practicable eliminar una actividad que está relacionada con objetivos para alcanzar fines sociales preestablecidos en la misión de la entidad.

– Reducir el riesgo

Implica llevar a cabo acciones para reducir la probabilidad o el impacto del riesgo o ambos conceptos a la vez. Esto implica típicamente a algunas de miles de decisiones cotidianas. Estas acciones se materializan en controles. Asimismo, la entidad puede diseñar planes de contingencias para actuar rápidamente y mitigar los impactos o consecuencias.

– Compartir el riesgo

La probabilidad o el impacto del riesgo se reduce trasladando o, de otro modo compartiendo una parte del riesgo. Habitualmente la transferencia del riesgo se realiza contratando pólizas de seguro o mediante el outsourcing de algunas operaciones, o tercerización de una actividad. Generalmente estas alternativas tienen un costo financiero.

En esta alternativa se considera la posibilidad de transferir el riesgo a otra unidad mediante atomización o desconcentración siempre que la unidad receptora de las operaciones o bienes riesgosos presente mejores condiciones para el tratamiento del riesgo; de lo contrario, la entidad no disminuirá su nivel de riesgo global.

– Aceptar el riesgo

No se toma ninguna acción para afectar la probabilidad o el impacto del riesgo.

Esta alternativa es aplicable cuando:

- Las probabilidades y/o los impactos son bajos.
- No es posible evitar ni reducir o transferir el riesgo.
- Los costos son injustificados respecto de los beneficios.

Si la entidad decide aceptar el riesgo debe monitorear continuamente las circunstancias que puedan hacer variar el nivel de riesgo.

En la Figura 17 se muestra la matriz de respuesta al riesgo mostrando las 9 alternativas o posibles grupos de respuesta en función al nivel de riesgo.

Nivel	Probabilidad	NR	Posibles Respuestas	NR	Posibles Respuestas	NR	Posibles Respuestas
3	Probable	3 Medio	Reducir Transferir	6 Alto	Evitar Reducir Transferir	9 Muy alto	Evitar Reducir Transferir
2	Posible	2 Bajo	Aceptar Reducir	4 Medio	Reducir Transferir	6 Alto	Evitar Reducir Transferir
1	Remoto	1 Muy bajo	Aceptar	2 Bajo	Reducir	3 Medio	Reducir Transferir
Impacto		Poco significativo		Significativo		Muy significativo	
Nivel		1		2		3	

Figura 17 Matriz de Respuesta al Riesgo

En función al Nivel de Riesgo se debe tomar las decisiones correspondientes de acuerdo a:

CAPITULO II Marco Conceptual, Teórico y Legal

– **Muy Alto:**

Es conveniente evitar el riesgo inmediatamente, alternativamente se debería reducir y/o transferir mediante decisiones de implementación inmediatas.

– **Alto:**

Es conveniente evitar el riesgo lo antes posible; alternativamente se debería reducir y/o transferir implementando acciones con plazos reducidos.

– **Medio:**

Es conveniente reducir y/o transferir el riesgo implementando acciones en el corto plazo.

– **Bajo:**

Cuando el impacto es poco significativo se podría aceptar el riesgo pero debido a una frecuencia posible es conveniente que alternativamente se procure reducir dicho riesgo en el corto plazo.

Cuando la probabilidad es remota pero el impacto es significativo, es conveniente reducir el riesgo implementando acciones en el corto plazo.

– **Muy Bajo:**

Se puede aceptar el riesgo debido a la probabilidad de remota de ocurrencia y al impacto poco significativo de su materialización.

Planificar el Tratamiento

Control	Medio
Planificar el tratamiento	– Análisis de la relación costo-beneficio. – Análisis del riesgo residual. – Mapa de Riesgos.

Planificación del tratamiento de los riesgos

Para planificar el tratamiento de los riesgos la entidad debe analizar las respuestas en el marco del costo-beneficio y el riesgo residual a efectos de elaborar el mapa de riesgos

Responsables de la Planificación

El análisis de la relación de costo-beneficio y del riesgo residual; como también, la elaboración del Mapa de Riesgos deben ser realizados por la unidad responsable de Gestión de Riesgos con el apoyo de las áreas y unidades organizacionales relacionadas con los riesgos. Dichos análisis deben estar debidamente documentados y juntamente al Mapa de Riesgos deben ser aprobados por el Comité de Gestión de Riesgos de la entidad.

Tareas para la Planificación de Tratamiento de Riesgos

Para el análisis del costo-beneficio se deben realizar, al menos, las siguientes tareas:

- Determinar los costos directos de las acciones a implementar. Generalmente estos costos están relacionados con tiempos de elaboración y otros insumos necesarios como recursos materiales o contrataciones específicas (seguros, especialistas, etc.).
- Procurar estimar los costos indirectos asociados con la distracción de algunos servidores públicos para las tareas de diseño de controles.
- Estimar los beneficios directos e indirectos a través de la magnitud de los perjuicios que se generarán por no implementar las acciones correspondientes.

En la mayoría de los casos los costos y los beneficios no son tangibles. Normalmente, los mayores beneficios (sociales, reputación o imagen institucional, etc.) no son cuantificables. En estas circunstancias se aplicará un criterio cualitativo consistente para poder comparar las opciones de respuesta.

CAPITULO II Marco Conceptual, Teórico y Legal

Para el análisis del riesgo residual se deben realizar, al menos, las siguientes tareas:

- Considerar los controles identificados e incluidos en la Matriz de Configuración de Riesgos.
- Considerar la efectividad de los controles aplicados.
- Considerar si los controles aplicados están diseñados o son informales.
- Revisar el nivel del riesgo residual a partir de la consideración de los controles.

A continuación se muestra la tabla de decisiones relacionadas con el tratamiento del riesgo residual.

CUADRO DE DECISIONES SOBRE EL NIVEL DE RIESGOS

Información obtenida sobre los controles	Decisiones sobre el Nivel de Riesgo
Inexistencia de controles.	Se mantiene el NR del Riesgo Inherente
Existen controles diseñados pero no aplicados efectivamente	Se mantiene el NR del Riesgo Inherente
Existen controles informales que se aplican efectivamente	La estimación del NR debe disminuir aunque no se considera neutralización total por la incertidumbre en su aplicación continua
Controles diseñados con aplicación efectiva	El NR residual es bajo.

1.5 Mapa de Riesgos

El mapa de riesgos en general es un instrumento informativo dinámico que permite conocer toda la información de los factores de riesgo y los probables efectos o consecuencias en una entidad así como la valoración, controles para su tratamiento.

El mapa de riesgos contiene a nivel estratégico los mayores riesgos a los cuales está expuesta la entidad, permitiendo conocer las políticas inmediatas de respuesta ante ellos

tendientes a evitar, reducir, compartir o transferir el riesgo; o asumir el riesgo residual, y la aplicación de acciones, así como los responsables, el cronograma y los indicadores.

No obstante se considera recomendable, elaborar un mapa de riesgos por cada proceso para facilitar la administración del riesgo, el cual debe elaborarse al finalizar la etapa de Valoración del Riesgo.

Para la elaboración del Mapa de Riesgos que incluya el plan de implementación se deben realizar, al menos, las siguientes tareas:

- Identificar los riesgos sujetos a tratamiento.
- Considerar las causas y las fuentes de los riesgos.
- Establecer las propuestas de tratamiento.
- Considerar el costo-beneficio de las propuestas de tratamiento.
- Considerar el riesgo residual sobre la base de los controles identificados para el riesgo.
- Mencionar las acciones necesarias para el tratamiento.
- Indicar el área o unidad y el responsable de la implementación de las acciones.
- Establecer el cronograma de implementación considerando las prioridades inherentes al nivel de riesgos, los recursos necesarios y los tiempos de desarrollo.

A manera de ejemplo se presenta un formato de Mapa de Riesgos según la Guía G/CE-021:

Area:		(1)		Elaborado por:		(3)		Fecha:		(5)
Unidad:		(2)		Aprobado por:		(4)		Fecha:		(6)
Riesgo	Impacto	Probabilidad	NR	Control existente	Riesgo residual	Propuestas de tratamiento	Acciones	Responsables	Cronograma	
(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)	

Características del Mapa de Riesgos:

- (1) Área: Identificar el Área Organizacional según el Manual de Organización y Funciones y el Organigrama vigente.

CAPITULO II Marco Conceptual, Teórico y Legal

- (2) Unidad: Identificar la unidad organizacional de acuerdo con el Manual de Organización y Funciones y el Organigrama vigente.
- (3) Elaboración: Identificar el funcionario que elabora el Mapa de Riesgos dependiente de la unidad encargada de coordinar la Gestión de Riesgos de la entidad.
- (4) Aprobación: Identificar el responsable jerárquico representante del Comité de Riesgos que aprueba el Mapa de Riesgos de la entidad.
- (5) Fecha de elaboración: Mencionar la fecha de emisión del Mapa de Riesgos.
- (6) Fecha de aprobación: Mencionar la fecha de aprobación por el Comité de Riesgos.
- (7) Riesgos: Incluir los riesgos del Área y Unidad que deben ser tratados.
- (8) Impacto: Mencionar la calificación a la o las consecuencias.
- (9) Probabilidad: Mencionar la calificación a la probabilidad de ocurrencia.
- (10) Nivel de Riesgo: Mencionar el NR de acuerdo con la Matriz de Respuesta al Riesgo.
- (11) Control existente: Si existiere, identificar el control diseñado o aplicado.
- (12) Riesgo residual: Establecer el NR considerando el efecto del control diseñado o aplicado.
- (13) Propuesta de tratamiento: Establecer la propuesta de tratamiento.
- (14) Acciones: Determinar las acciones que se deben realizar para implementar la propuesta de tratamiento.
- (15) Responsable: Establecer el Área o unidad organizacional y el responsable de implementar las acciones para el tratamiento del riesgo.
- (16) Cronograma: Establecer el cronograma de implementación.

CAPITULO III MANUAL DE RIESGO OPERATIVO

De acuerdo a lo explicado en el marco conceptual y teórico, el estudio así como la gestión de los riesgos operativos no es un tema reciente, actualmente los modelos de gestión empresarial han evolucionado desde los modelos de control interno COSO, COSO ERM y la norma de Administración de Riesgos de la Entidad INTOSAI GOV 9130, hasta llegar a lo que es la Gestión del Riesgo conforme a la ISO 31000 basada en la norma AS/NZS 4360:2004 mediante la creación del marco conceptual técnico de una disciplina denominada “Administración de Riesgos” o “Gerencia de Riesgos” que es una función de muy alto nivel y se ha convertido en vital para cualquier organización con el objeto definir un conjunto de políticas y estrategias que a partir de los recursos (físicos, humanos y financieros) busca en el corto plazo mantener la estabilidad financiera de la empresa, protegiendo los activos e ingresos y en el largo plazo, minimizar las pérdidas ocasionadas por la ocurrencia de dichos riesgos, si bien en el ámbito privado su fin final es generar valor para los dueños o accionistas de las empresas, para el sector público se traduce en generar valor público con la otorgación de servicios o bienes para la sociedad.

Sin embargo, en el estado Boliviano, no se cuenta con una política de estado o de gestión gubernamental sobre la Administración de Riesgos tendiente a darle un manejo adecuado a los riesgos con el fin de lograr de la manera más eficiente el cumplimiento de sus objetivos y estar preparados para enfrentar cualquier contingencia que se pueda presentar. Simplemente se ha realizado una aproximación a la gestión del riesgo a través de los Principios, Normas Generales y Básicas de Control Interno Gubernamental CI/08 de la gestión 2000 y su norma secundaria la Guía de Implantación del Control Interno G/CE-21 de la gestión 2008 se adopta el Modelo de Control Interno COSO para aplicación por todas las entidades del Sector Público sujetas a la implantación del proceso de control interno, conforme establece el artículo 22° del Reglamento para el Ejercicio de las Atribuciones de la Contraloría General de la República aprobado mediante Decreto Supremo N° 23215.

En el entendido que el sector público Boliviano no puede estar exento de la tendencia moderna de gestión sobre Administración de Riesgos, y no es un tema nuevo para las entidades públicas, debido a que las normas secundarias emitidas por la Contraloría General del Estado sobre la implantación del control interno gubernamental ya establecen guías para la evaluación de riesgos como mecanismo de control para limitar los riesgos internos y externos, desde un enfoque de control y no así de gestión de riesgos para aplicación de todas las entidades de la Administración Pública, con el fin de lograr de la manera más eficiente el cumplimiento de sus objetivos y estar preparados para enfrentar cualquier contingencia que se pueda presentar.

En este sentido, las entidades de la Administración Pública Financiera no Bancarias no pueden ser ajenas al tema de los riesgos y deben buscar cómo manejarlos y controlarlos, partiendo de la base de su razón de ser y de su compromiso con la sociedad, por esto se debe tener en cuenta que los riesgos no solo son de carácter económico y están directamente relacionados con el logro de los objetivos institucionales de las entidades financieras no bancarias cuyo objetivo final es contribuir al desarrollo del país generando valor público con los servicios prestados a través del financiamiento que otorgan.

Debido que la gestión del riesgo operativo inicialmente ha sido planteado para entidades financieras debido al efecto que estos pueden generar en caso de pérdidas es que el Comité de Basilea emite los principios y las buenas prácticas, por lo otro lado la norma INTOSAI GOV 9130 de la INTOSAI sobre la Administración de Riesgos es más genérico para su aplicación en entidades públicas y aún más se estandariza la gestión del Riesgo con las normas AS/NZS 4360:2004 y la ISO 31000:2009 de Administración y Gestión del Riesgo respectivamente.

El ámbito de aplicación del presente proyecto es el Sector Público Financiero no Bancario del universo de la Administración Publica Nacional de Acuerdo a la Figura 18,

para la gestión 2012 es parte de la Administración Pública Financiera de acuerdo a las Directrices de Formulación Presupuestaria de 2012.

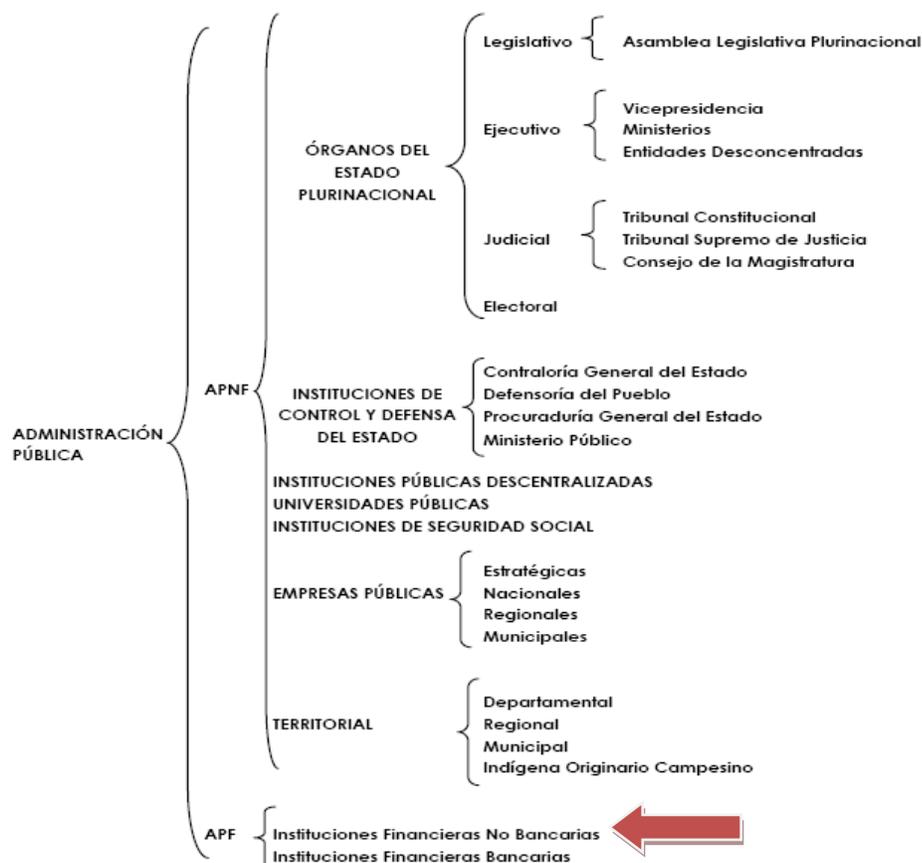


Figura 18 Ámbito del Sector Público

En ese entendido las Entidades Públicas Financieras no Bancarias que podrían aplicar e implementar el presente proyecto son:

1. Fondo de Inversión Productivo y Social (FPS)
2. Fondo de Desarrollo del Sistema Financiero y de Apoyo al Sector Productivo (FONDESIF)
3. Fondo De Financiamiento para La Minería (FOFIM)
4. Fondo Nacional de Desarrollo Regional (FNDR)
5. Fondo Nacional de Desarrollo Alternativo (FONADAL)

6. Fondo de Desarrollo para los Pueblos Indígenas, Originarios y Comunidades Campesinas (FDPIOCC)

7. Otras entidades que tengan el ciclo operativo financiero similar.

Se ha seleccionado este tipo de entidades debido a que a diferencia de las entidades Financieras Bancarias estas se encuentran reguladas por la ASFI por lo tanto la Gestión del Riesgo Operativo es una obligación su implantación en el mediano plazo conforme al marco regulatorio para entidades de supervisión financiera descritos en Basilea II.

Las Entidades del Sector Público Financiero no Bancario, no están sujetas a ningún marco regulatorio ya que su fin como dice su denominación es financiero sin recurrir a la intermediación financiera de recursos públicos, más bien realizan una canalización de recursos externos e internos para el financiamiento de proyectos de inversión pública sea de carácter social o productivo.

El Artículo 10 de las Normas Básicas del Sistema de Crédito Público define el rol de las Entidades Financieras No Bancarias del Sector Público Boliviano de acuerdo a lo siguiente:

“Las Entidades Financieras No Bancarias del Sector Público, en el ámbito de su competencia, tendrán a su cargo la canalización o ejecución de los recursos externos contratados por la República y transferidos para su administración mediante Convenios Subsidiarios.

Las Entidades Financieras No Bancarias del Sector Público, en calidad de entidades ejecutoras y/o deudoras deberán asegurar la disponibilidad de información actualizada, oportuna y confiable sobre la administración de los recursos transferidos, en términos de su recepción- destino- reembolso, a efectos de su análisis, seguimiento y control”.

Por otro lado, este tipo de entidades de acuerdo al ámbito de sus competencias de manera genérica tienen un mismo ciclo operativo y financiero de acuerdo a la Figura 19.

El ciclo operativo y financiero de las Entidades Financieras no Bancarias del Sector Público es la base conceptual y operativa que refleja la razón de ser estas entidades así como su macro funcionamiento, este comprende 4 etapas básicas de acuerdo a la Figura 19 estas son Captar, Colocar, Recuperar y Pagar el Servicio de la Deuda (Pago a Organismos Financiadores) o la Reinversión de Recursos.

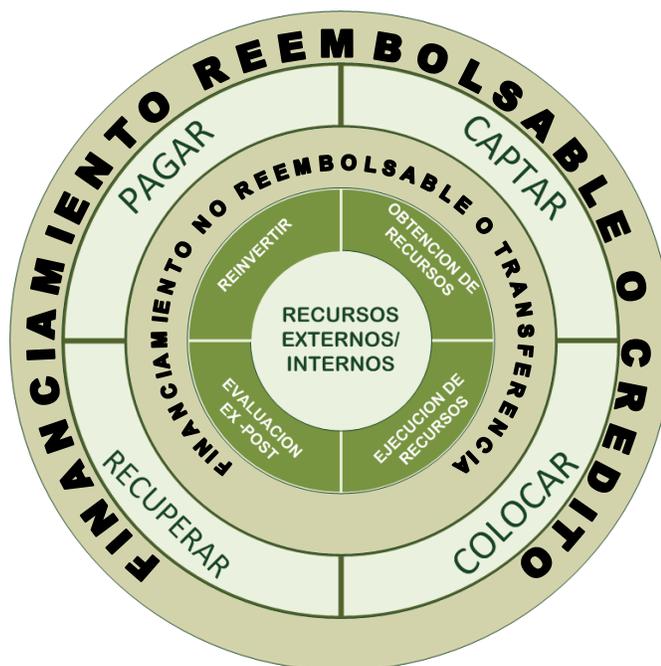


Figura 19 Ciclo Operativo y Financiero de las Entidades Financieras

a) Captación

La captación corresponde a actividades de obtención de recursos provenientes de fuentes externas o internas, destinadas a la colocación de las mismas en calidad de crédito o transferencia no reembolsable a favor de los Sujetos de Financiamiento para la ejecución de planes, programas o proyectos, en el ámbito de la competencia de la entidad financiera no bancaria.

Todo proceso de captación de recursos externos se origina en los diferentes contratos de préstamo o convenios que el país suscribe con los financiadores externos y que se instrumenta con el propósito de particularizar a nivel de cada entidad con la firma de los respectivos convenios subsidiarios, en base a los cuales se establecen las condiciones técnicas y financieras de cada programa o línea de financiamiento.

b) Colocación

La colocación es la fase o etapa en la que la entidad financiera no bancaria realiza la ejecución en calidad de crédito y/o transferencia a los beneficiarios o sujetos de financiamiento conforme a las condiciones establecidas en los convenios subsidiarios de cada programa y línea de financiamiento obtenida.

El marco legal para la colocación de recursos es un Contrato de Préstamo o Convenio de Transferencia de Recursos suscrito entre la entidad Financiera no Bancaria y beneficiario o sujeto de financiamiento donde se especifican condiciones financieras referidas a monto, plazo, periodo de gracia, interés, garantías y otras que conlleva la deuda que está adquiriendo el sujeto de Financiamiento en caso de crédito.

Los recursos para la captación puede provenir directamente de la captación o ser producto de excedentes institucionales como recursos propios destinados a la reinversión de los mismos, en todos los casos el destino de los mismos son para beneficiario o sujetos financiamiento para la ejecución de planes, programas y

proyectos para coadyuvar el cumplimiento de objetivos establecidos en el Plan Nacional de Desarrollo (PND) y otras priorizadas por el Estado Plurinacional.

La colocación de recursos conlleva un Proceso de financiamiento, que ha sido diseñado para que este sea ágil y oportuno a las necesidades de beneficiarios o Sujetos de Financiamiento y conforme a la normativa interna de cada Entidad Financiera no Bancaria.

c) Recuperación

La recuperación es el proceso de cobros realizado por la entidad Financiera no Bancaria a los beneficiarios o Sujetos de Financiamiento, conforme a las condiciones establecidas en sus contratos de préstamo o transferencia rembolsable en base a los cuales se produce el retorno del capital que dio origen al financiamiento. La Entidad Financiera no Bancaria está facultado para implantar los mecanismos que garantizan la recuperación del crédito y otros estipulados en el contrato.

d) Pagar el Servicio de la Deuda

Corresponde a la devolución de los recursos obtenidos en la fase de captación a los organismos financieros conforme a los contratos de préstamo suscritos cumpliendo con las fechas y plazos de vencimiento establecidos mediante las tablas de amortización por servicio de la deuda, siendo estos pagos realizados mediante el Banco Central de Bolivia entidad designada por el Estado Boliviano para canalizar estas obligaciones.

e) Re inversión

Es la etapa que re-utiliza los excedentes de los recursos obtenidos de la fase de recuperación en nuevos emprendimientos financieros mediante la creación de un programa para la ejecución de proyectos.

Luego de revisar el marco teórico y conceptual sobre la gestión de riesgos, una de las maneras más eficientes de lograr la adopción e integración en las entidades del Sector Público Financiero No Bancarias un modelo de gestión de riesgos, es mediante la aplicación de un proceso metodológico basado en un Marco de Gestión de Riesgo Operacional, tal cual lo describe la norma ISO 31000, pues esta mejora el modelo administración de riesgos de la norma AS/NZS 4360:2004 adicionándole el marco y los principios de la gestión de riesgos al proceso de gestión de riesgos, por otro lado, este documento mejora sustancialmente o significativamente a los modelos de evaluación de riesgos del informe COSO – ERM, Basilea II, Guía para las Normas del Control Interno del Sector Público de la INTOSAI y los Principios, Normas Generales y Básicas de Control Interno emitidos por la Contraloría General del Estado.

El enfoque general de estos modelos es diferente, pues tienen diferentes objetivos u orientaciones, que podrían dividirse en dos grupos de modelos de gestión de riesgo con las siguientes diferencias básicas.

CUADRO DE DIFERENCIAS GESTION DE RIESGO Y CONTROL

Norma ISO 31000 y AS/NZS 4360	Guía INTOSAI, MODELO COSO ERM, Principios, Normas Generales y Básicas de Control Interno (CGE)
<ul style="list-style-type: none">• La gestión del riesgo es integrada a los procesos.• Revisión continúa del modelo de gestión de riesgo.• Proceso simple de gestión de riesgo.• Se sistematiza la gestión de riesgos con la implantación de principios, el marco y el proceso de gestión de riesgos.• Gestión del Riesgo Preventivo.• Establece un contexto externo de la	<ul style="list-style-type: none">• No comprende a los riesgos como un proceso, sino como evaluación de riesgos.• La evaluación de riesgos se la hace periódicamente. (auditorias)• El proceso de evaluación es complejo.• No está estructurado es un modelo simple de evaluación de riesgos.• Modelo correctivo de control interno a través de la evaluación de riesgos.• Carece de contexto externo para la gestión de

gestión del riesgo.	riesgos.
---------------------	----------

La aplicación del marco debe comprender tres grandes etapas que se debe iniciar, fundamentalmente en la creación o fortalecimiento de una cultura de riesgo y control de todo el personal de la institución, luego se continúan con una etapa de diseño del marco de la gestión de riesgos donde se en la cual se establecen una adecuada estructura organizativa así como los procesos de gestión del riesgo, recursos, etc y la última etapa es la aplicación del Proceso de Gestión del Riesgo donde inicia con el establecimiento del contexto, análisis del riesgo

a) Cultura y Compromiso

Esta primera etapa adquiere significativa relevancia, ya que implica el convencimiento de alta dirección y/o Máxima Autoridad Ejecutiva (MAE) de los beneficios y la necesidad de implantar un marco que administre el riesgo operativo. Posteriormente, se debe fomentar una cultura positiva de riesgo en las unidades operativas, financieras y apoyo de las entidades, porque son estas las que manejan las operaciones y transacciones en el día a día.

Una cultura de riesgo y control se promueve con diversas acciones, entre las cuales se pueden mencionar charlas, cursos y talleres de capacitación, en los cuales se difunda en el personal la importancia de gestionar los riesgos como también dotarlos de herramientas y conocimientos que les facilite una participación proactiva en la gestión de los riesgos.

Adicionalmente, deben existir campañas de divulgación permanente, mediante boletines, correos electrónicos, información en las carteleras, paneles informativos, entre otros, en las cuales se comuniquen temas conceptuales, noticias, estrategias y beneficios de la gestión de riesgos.

Estas acciones tienen como propósito, además, el comunicar indirectamente al personal sobre el compromiso y la firme decisión de la Máxima Autoridad Ejecutiva en la implantación de medidas para proteger a las entidades de posibles eventos que generen incertidumbre en el logro de los objetivos.

b) Establecimiento del Marco de la Gestión de Riesgos

El establecimiento del Marco se traduce en proporcionar las bases y disposiciones que se implementaran en la entidad pública financiera no bancaria en todos los niveles.

El marco es la base de la gestión de los riesgos de manera efectiva, mediante la aplicación del proceso de gestión del riesgo en los diferentes niveles y dentro de los contextos específicos de cada entidad.

El marco garantiza que la información sobre los riesgos determinados en el proceso de gestión se informe adecuadamente y sea utilizado como base para la toma de decisiones y la rendición de cuentas en todos los niveles de cada entidad.

Este marco es la estructura de la gestión de riesgos incorporada en la estructura organizacional en cada entidad, por lo tanto cada entidad debe adaptarla de acuerdo a sus necesidades específicas. Esta adaptación mínima se encuentra en el manual de riesgo operativo, pues en este documento se determinan por ejemplo, la creación del comité de riesgos, de una unidad de gestión de riesgo y su relación con auditoría, establecimiento de políticas de riesgo, seguimiento y revisión continua de los procesos y del marco o estructura de la gestión de riesgos, la comunicación e información de toda la gestión de riesgo y por último la implantación de la gestión de riesgos.

c) Proceso de la Gestión de Riesgos

El proceso de gestión del riesgo a aplicar en las entidades públicas financieras no bancarias debe ser:

- Integral en la gestión institucional.
- Ser parte de la cultura y las buenas prácticas de gestión y control,
- Adoptados a los procesos operativos y administrativos de cada entidad.

Este proceso de la gestión de riesgos estará detallado en el manual de riesgo operativo.

A continuación se presenta la propuesta del diseño de un Manual de Riesgo Operativo, donde se establecen los principios, marco y proceso de la gestión de riesgos, para que se inicie el proceso de implementación de un proceso de gestión del riesgo operativo, identificando los riesgos operativos hasta su reducción al mínimo de los riesgos vinculados al ciclo financiero y operativo de las entidades públicas financieras no bancarias para disminuir la incertidumbre en el logro de los objetivos.

El contenido del manual de riesgo operativo es el siguiente:

6.1 **Introducción**

Las Entidades Públicas Financieras no Bancarias han venido desarrollando planes, programas y proyectos con el fin de lograr de la manera más eficiente el cumplimiento de sus objetivos y a su vez, buscando estar preparados para enfrentar las contingencias que se puedan presentar.

La gestión de riesgos es importante y a pesar de que no ha sido normado formalmente por alguna instancia gubernamental y no existe un entidad rectora de este tipo de gestión la entidad más cercana a este tema es la Contraloría General del Estado, se debe implantar un sistema de gestión de riesgos dependiendo del tamaño de la entidad, de la cultura organizacional, según la complejidad de sus operaciones y la disponibilidad de recursos.

El concepto de administración o gestión del riesgo en las entidades del Estado, considera la exposición permanente a diferentes riesgos que en un momento dado pueden poner en peligro su existencia y/o el cumplimiento de sus objetivos institucionales; en razón a ello, desde la perspectiva de los modelos y normas técnicas o estándares aplicados a la

gestión de riesgos, se interpreta que la eficiencia del control, o su principal propósito, es la reducción de los riesgos, por lo tanto la gestión de riesgos se considera como la evolución del enfoque de control interno Gubernamental que se aplica conforme a la Ley 1178.

Las Entidades Públicas Financieras no Bancarias, tienen la responsabilidad de diseñar y aplicar métodos y procedimientos de Control Interno, que permitan identificar y evaluar los eventos internos y externos que pueden afectar o impedir el normal desarrollo de los procesos y el cumplimiento de los objetivos institucionales.

Dentro de estos criterios, corresponde administrar los riesgos, a partir de la adopción del Mapa de Riesgos y el Plan de Manejo de los Riesgos, el cual es concebido como una herramienta de gestión establecida para minimizarlos, monitorearlos y corregirlos y así evitar la extensión de sus efectos, bajo parámetros de calidad, eficiencia, economía y eficacia.

El Mapa de Riesgos y el Plan de manejo de los Riesgos que se describen en el presente documento son producto de gestión de riesgos bajo la estructura de un enfoque por procesos, adicionalmente es el producto de un trabajo colectivo de los Comisionados, Máxima Autoridad Ejecutiva, Directores, Jefes de Área, Asesores, y demás servidores públicos vinculados a la Entidad, quienes participaron en la elaboración e implementación del Mapa y Plan de Manejo de los Riesgos de las áreas.

El documento incluye los principios y la política Institucional de la administración del riesgo, las políticas operativas, su comunicación, así como el marco conceptual y legal sobre el cual se soporta. Adicionalmente se describe la estructura o marco de la gestión de riesgos que se traducen en la creación de las unidades de gestión de riesgos, el comité de riesgos, los procedimientos, obligaciones y responsabilidades para la gestión del riesgo.

En este documento también se describe el proceso de la gestión del riesgo, responsables, sus procedimientos, metodología de la gestión del riesgo en base al enfoque ya definido en la política de gestión del riesgo.

6.2 Principios de la Gestión de Riesgos

La Entidad Pública Financiera No Bancaria establece los siguientes principios para la gestión de riesgos y que tienen que ser aplicados en todos los niveles de la entidad e implantados dentro de la cultura organizacional:

i. La gestión de riesgo crea y protege el valor.

La gestión del riesgo debe contribuir a la consecución de los objetivos institucionales y de área funcional mejorando el rendimiento en todas las áreas como por ejemplo la seguridad jurídica, el cumplimiento de normas legales, aceptación de clientes internos y externos, la calidad de servicios, gestión de financiamiento de proyectos, la eficiencia en las operaciones, el buen gobierno, aceptación del control social y la reputación o prestigio institucional.

ii. Debe ser parte integral de todos los procesos de la entidad.

La gestión de riesgos no es una actividad aislada, separada de las principales actividades y procesos de la entidad. Debe ser parte integrante de todos los procesos de la entidad y ser incluida en la planificación estratégica.

iii. La gestión de riesgos es parte de la toma de decisiones.

La gestión de riesgos debe ayudar a los ejecutivos de las entidades que toman las decisiones, para priorizar acciones y determinar los cursos alternativos de acción.

iv. Se basa explícitamente en la incertidumbre.

La gestión de riesgos se basa explícitamente en la incertidumbre, el efecto de esa incertidumbre en el logro de los objetivos.

v. La gestión de riesgos debe ser sistemática, estructurada y oportuna.

La entidad debe adoptar un enfoque sistemático, oportuno y estructurado para la gestión del riesgo, que contribuya a la eficiencia y lograr resultados consistentes, comparables y fiables.

vi. La gestión de riesgos se basa en la mejor información disponible.

La información de entrada para el proceso de gestión de riesgos se basa en datos históricos, la experiencia en riesgos tolerados, información de interesados o terceros, la observación, pronósticos e informes de auditoría.

vii. La gestión del riesgo toma en cuenta los factores humanos y culturales.

La gestión del riesgo reconoce las capacidades, las percepciones y las intenciones de los servidores públicos que puede facilitar u obstaculizar el logro de los objetivos de la entidad.

viii. La gestión del riesgo debe ser transparente e inclusivo.

La adecuada y oportuna participación de los interesados, control social y, en particular los tomadores de decisiones en todos los niveles de la entidad, asegura que la gestión del riesgo sea pertinente y actualizada. También debe permitir que sus criterios u opiniones sean tomados en cuenta en la determinación del riesgo.

ix. La gestión de riesgos es dinámica, interactiva y de respuesta al cambio.

La gestión de riesgos es mejorada continuamente y responde a los cambios. Los cambios en acontecimientos externos e internos, el cambio del contexto institucional, el seguimiento y revisión de los riesgos pueden originar nuevos riesgos, algunos cambian y otros desaparecen.

x. La gestión de riesgos facilita la mejora continua de la organización.

La entidad debe desarrollar y aplicar estrategias para mejorar su madurez de gestión de riesgos, conjuntamente a los demás aspectos de su organización para una mejora continua.

6.3 **Políticas Institucionales de Administración del Riesgo**

Las políticas identifican las opciones para tratar y manejar los riesgos basados en la calificación y evaluación de los mismos, lo cual permite la toma de decisiones adecuadas y facilita fijar los lineamientos de la administración del riesgo.

Basado en lo anterior, la entidad se compromete a establecer acciones preventivas a eventos que pongan en riesgo el normal desarrollo de los procesos requeridos para el cumplimiento de los objetivos de la entidad. Asimismo, se compromete a preservar la eficacia operativa de la entidad, así como con la salvaguarda y bienestar de sus funcionarios, garantizando el mejor manejo de los recursos mediante el establecimiento e implementación de un Sistema de Administración del Riesgo que permita la minimización de los costos causados por estos.

La Entidad Pública Financiera no Bancaria establece las siguientes políticas para la administración del riesgo:

- Determinar en base a la valoración del riesgo las decisiones acerca de su tratamiento dentro del rango d: Evitar el riesgo, Reducir el riesgo, Compartir o Transferir el riesgo u Asumir un riesgo.
- Aceptar una tolerancia de riesgo frente a cada proceso de manera individual y general hasta el nivel de moderado, por tanto los riesgos enmarcados dentro del nivel de importantes e inaceptables serán prioridad de tratamiento.
- En la fijación de opciones para el tratamiento de los riesgos, éstos se evaluarán en términos de su relación costo / beneficio.
- Anualmente se reformularán, dentro de los primeros 60 días, el plan de manejo de los riesgos, estableciendo los nuevos riesgos y las acciones para su tratamiento.
- Se establecerá dentro de la concertación de objetivos, acuerdos de gestión, planes, programas y proyectos el análisis, valoración y manejo de los riesgos.
- Generar en cada uno de los servidores públicos una cultura de administración de los riesgos para asegurar el reconocimiento de los riesgos y las oportunidades que se

presentan, creando conciencia de que si no se administran apropiadamente pueden afectar el logro de los objetivos.

Además velará por la oportuna identificación de eventos o situaciones que afecten negativamente la entidad y la valoración de los riesgos, así como la selección de una metodología para su tratamiento y monitoreo, de tal manera que procure evitar la materialización de eventos generadores que puedan afectar el cumplimiento de los lineamientos estratégicos de la entidad.

Comunicación y adoctrinamiento de la Política

A fin de establecer e implementar el marco o la infraestructura y el compromiso necesario para asegurar que la administración del riesgo se convierta en parte integral de la planeación y de los procesos, se desarrollarán planes de capacitación, así como efectuar las publicaciones que sean necesarias para lograr la interiorización y sensibilización de los servidores públicos hacia el tema de la administración del riesgo.

6.4 Estructura, Funciones y Responsabilidades

Para implementar el enfoque y metodología de riesgos es necesaria la creación de unidades relacionadas a la gestión de riesgos dentro del marco de la gestión de riesgos.

6.5 Responsabilidad del Directorio o Comités Ejecutivos

El Directorio o Comités Ejecutivos (DCE) es el órgano que define políticas institucionales, coordina, norma y fiscaliza de las entidades públicas financieras no bancarias, incluyendo la revisión de planes, cambios en la estructura organizacional, políticas generales y de control. Dentro de esto último está el de establecer los límites sobre la exposición al riesgo total que enfrenta las entidades.

Las responsabilidades de este órgano deben considerar adicionalmente:

- a) Aprobar las políticas, procedimientos y mecanismos orientados a generar un sistema adecuado de administración y control de riesgos operativos. Estas medidas han de

incluir la oportunidad, frecuencia y tipo de informes a recibir por los miembros del DCE.

- b) Designar a los miembros del Comité de Riesgos, preferentemente con antecedentes o capacitación necesaria.
- c) Conformar una Unidad de Riesgos bajo la responsabilidad de un funcionario que cumpla el perfil profesional en el área de riesgos y con los requisitos que exige este documento.
- d) Aprobar las funciones y responsabilidades de las unidades encargadas de la administración, control y monitoreo de riesgo.
- e) Asegurar que la Unidad de Riesgos desarrolle sus funciones con absoluta independencia técnica de acuerdo con las disposiciones establecidas en la presente norma.
- f) Asegurar que las unidades de gestión de riesgos implementen y ejecuten las disposiciones establecidas en políticas y procedimientos emanados por el Directorio o Comité Ejecutivo.
- g) Aprobar los planes y funciones de la Auditoría Interna relativas a verificar la ejecución de las políticas y procedimientos aprobados para la adecuada gestión del riesgo.

La responsabilidad del Directorio o Comité Ejecutivo abarcara también la vigilancia de la difusión de la cultura de riesgos, valores y gestión institucional.

6.5.1 Comité de Riesgos

Toda Entidad Pública Financiera no Bancaria debe contar con un Comité de Riesgos conformado por lo menos por una autoridad Jerárquica (Gerente o Director de área), quien lo preside, Directores o Gerentes de Área, Responsable de la Unidad de Riesgos y Jefes de Unidad conforme a las instrucciones del Directorio, Comités Ejecutivos o instancia de Tuición o Control.

6.5.1.1 Obligaciones del Comité de Riesgos

El Comité de Riesgos es el órgano técnico especializado y responsable de la administración de los riesgos, en cuanto al diseño de las políticas, sistemas, metodologías, modelos y procedimientos para la eficiente administración de los riesgos que enfrenta la entidad pública financiera no bancaria y los límites de exposición, a los que se encuentran expuestos.

De la misma manera, el Comité deberá establecer los canales de comunicación efectivos con el fin que las áreas involucradas en la toma, registro, identificación y administración de riesgos tengan conocimiento de los riesgos asumidos.

6.5.1.2 Funciones

Las funciones del Comité de Riesgos en forma genérica son:

- a) Proponer para la aprobación del CE o Directorio los Planes Anuales y el Manual de Control de Riesgos que contenga los objetivos, políticas y procedimientos para la administración integral de riesgos.
- b) Proponer para la aprobación del Directorio los límites de exposición al riesgo de manera global y por tipo de riesgo.
- c) Proponer la evaluación de riesgos de nuevas operaciones, planes o programas que la entidad planea crear.
- d) Participar en la evaluación de la contratación del responsable de la Unidad de Riesgos.
- e) Informar periódicamente al Directorio o Comité Ejecutivo y cuando lo considere conveniente, sobre la exposición al riesgo asumido por la Entidad Financiera no Bancaria y de los efectos negativos que se podrían producir, así como sobre el cumplimiento de los límites de exposición a los riesgos establecidos.
- f) Informar al Directorio sobre las medidas correctivas implementadas, tomando en cuenta el resultado de las auditorías y evaluaciones relativas a los procedimientos de administración de riesgos.

g) Crear los subcomités que se consideren convenientes para el ejercicio de sus funciones.

6.5.1.3 Modificación de Límites

El Comité de Riesgos previa aprobación del Directorio o Comité Ejecutivo, podrá ajustar los límites cuando estos excedan los límites de exposición a los distintos tipos de riesgo cuando las situaciones y el entorno así lo requieran.

6.5.1.4 Reuniones del Comité de Riesgos

El Comité de Riesgos deberá reunirse con la periodicidad que establezca su reglamento interno de trabajo. En dichas reuniones participarán los funcionarios que el Comité de Riesgos considere necesarios.

Todas las sesiones y acuerdos del Comité de Riesgos deberán registrarse en una bitácora de reuniones debidamente suscrito por todos y cada uno de sus integrantes, documento que estará a disposición de las instancias de control posterior y el Directorio o Comité Ejecutivo.

6.5.1.5 Reglamento Interno de Trabajo del Comité de Riesgos

El Comité de Riesgos es el encargado de elaborar el reglamento interno de trabajo que será aprobado por el Directorio o Comité Ejecutivo. Contendrá los procedimientos para el cumplimiento de sus funciones conforme a las políticas de gestión de riesgos vigente. Dicho reglamento establecerá, entre otros aspectos, la periodicidad de sus reuniones así como la información que deberá ser remitida a la directiva.

6.5.1.6 Requisitos de los Miembros del Comité de Riesgos

El Comité de Riesgos debe estar compuesto por miembros que cuenten con un amplio conocimiento en materia de identificación, monitoreo, control y estimación de riesgos, en caso de no contar con personal calificado en el tema de riesgos, es responsabilidad de la Entidad Pública Financiera no Bancaria la capacitación suficiente en el área de riesgos operativos.

6.5.1.7 Periodo de Vigencia

El plazo de vigencia del Comité de Riesgos es por un periodo mínimo de dos años, siempre que su mandato no expire antes u otros casos debidamente fundados, y un máximo de cuatro años. La renovación sólo incluye al presidente del Comité.

6.5.2 UNIDAD DE RIESGOS

La Unidad de Riesgos es una unidad autónoma, que deberá ser independiente de las áreas de sustantivas u operativas y del área administrativa, a fin de evitar conflictos de intereses y asegurar una adecuada separación de responsabilidades. Su tamaño y ámbito deberán estar en relación con el tamaño y la estructura de la entidad y con el volumen y complejidad de los riesgos en los que incurre. El Comité de Riesgos deberá establecer las funciones específicas de esta Unidad dentro de la estrategia institucional.

6.5.2.1 Funciones

La Unidad de Riesgos es la encargada de:

- a) Identificar, monitorear, controlar y estimar los riesgos que enfrenta la Entidad Pública Financiera no Bancaria en todas sus dependencias y oficinas regionales.
- b) Participar en el diseño y permanente adecuación del manual de organización y funciones, de políticas y procedimientos de control de riesgos.
- c) Informar al Directorio, comités y áreas de decisión, sobre los riesgos, los grados de exposición y la administración de éstos, de acuerdo a las políticas y procedimientos establecidos por la entidad.

6.5.2.2 Recursos Materiales de la Unidad de Riesgo

El Directorio o Comité Ejecutivo debe asegurar que la Unidad de Riesgos cuente con una infraestructura adecuada, así como con recursos humanos, técnicos y logísticos de acuerdo con la naturaleza de sus actividades.

Estos deben guardar relación con la magnitud y complejidad de las operaciones y estructura de la entidad en sus programas de financiamiento y los riesgos que enfrenta.

El responsable de la Unidad de Riesgos y los integrantes de esta unidad deben recibir capacitación permanente en materias relacionadas a sus funciones.

6.5.2.3 Comunicaciones de la Unidad de Riesgo con Auditoría Interna

Con la finalidad de evaluar permanentemente el funcionamiento de los sistemas de gestión de riesgo, la Unidad de Riesgos deberá establecer las comunicaciones necesarias con auditoría interna. El Responsable de la Unidad, coordinará reuniones periódicas con esta unidad, en las que se tratarán temas de mutuo interés, intercambio de reportes y otros documentos, así como del entendimiento y aplicación de técnicas, métodos y terminologías comunes. Las comunicaciones que se establezcan se realizarán bajo la observancia de la normativa vigente.

6.5.3 JEFE O RESPONSABLE DE LA UNIDAD DE RIESGOS

6.5.3.1 Responsabilidad

El responsable de la Unidad de Riesgos tiene como labor la identificación, monitoreo, control y estimación de los riesgos que enfrenta la entidad de intermediación financiera en las diversas actividades de negocio. Debe elaborar informes sobre la gestión del riesgo global y riesgos individualizados a ser enviados al Comité de Riesgos, al Directorio y a la Gerencia General, así como preparar reportes periódicos correspondientes.

6.5.3.2 Funciones

Las funciones mínimas del responsable de la Unidad de Riesgos son:

- a) Difundir la cultura de gestión de riesgo en la entidad.
- b) Diseñar e implementar el sistema, metodología, métodos y modelos de medición de riesgos y reportes. Esto incluye el reservorio de aquella información sobre pérdidas, exposiciones al riesgo, mecanismos de detección temprana de riesgos entre otros eventos.

- c) Hacer seguimiento para verificar el adecuado cumplimiento del manual de riesgo operativo en cuenta a la gestión del riesgo.
- d) Establecer las escalas de valoración de probabilidad y consecuencia de los riesgos.
- e) Coordinar con las áreas operativas y administrativas en lo referente a la correcta identificación, monitoreo, control y estimación de riesgos.
- f) Ejecutar los procesos de auto evaluación para la adecuada comprensión del proceso e identificación de riesgos junto a las unidades de negocio y apoyo.
- g) Proponer una vez identificadas las necesidades de capacitación sobre temas relativos a la administración de riesgos.
- h) Implantar el modelo de gestión de riesgo bajo el enfoque y metodología del Manual de Riesgo Operativo.
- i) Analizar, revisar y reportar el comportamiento de la relación riesgo-retorno a través del control y monitoreo de las actividades de la entidad y de las estrategias aplicadas por la Dirección Ejecutiva o Gerencia General y del costo-beneficio de incrementar, aceptar, retener, evitar, financiar y/o transferir el riesgo
- j) Desarrollar sistemas analíticos y con una alta capacidad de gestión de datos que respalden al programa o plan de gestión global de riesgos.
- k) Elaborar informes y reportes específicos sobre la gestión de riesgos.
- l) Participar con voz y voto en el Comité de Riesgos y en la aprobación de operaciones que realicen las unidades y áreas funcionales de este manual.

6.5.3.3 Requisitos del Responsable de la Unidad de Riesgos

Al seleccionar al Jefe o responsable de la Unidad de Riesgos, el CD debe asegurar requisitos de: solvencia moral, conocimientos y experiencia apropiados para la función que desarrolla en dicha unidad, debiendo reunir los siguientes requisitos mínimos:

- a) Tener una experiencia en actividades de gestión de riesgos en entidades de intermediación financiera o no financieras.
- b) Tener título profesional en materias afines.

- c) Acreditar conocimiento de normas, reglamentos, políticas y mejores prácticas en la gestión de riesgo, entre otros.
- d) Acreditar capacitación permanente en las materias mencionadas en c).
- e) Dedicación exclusiva al cargo dentro de la entidad de intermediación financiera.

6.5.3.4 Impedimentos

- a) Estar en situaciones que limiten la necesaria independencia para el ejercicio de sus funciones o que contravengan las normas de personal de la entidad.
- b) Estar incurso en alguno de los impedimentos señalados por la normativa legal vigente.
- c) En caso que las funciones de Riesgos sean terciarizadas, quedarán impedidos de ejercer esta función las firmas de consultoría o auditoría externa o cualquier otro asesor que tenga contrato vigente.

6.5.4 DE LA UNIDAD DE AUDITORÍA INTERNA

Se complementaran las funciones de auditoria interna con lo siguiente:

- a) Evaluar el cumplimiento de los procedimientos utilizados para la administración de riesgos.
- b) Proporcionar la información sobre eventos de pérdida registrados como input para las auto evaluaciones durante el proceso de gestión del riesgo.
- c) Proporcionar la información sobre las observaciones y recomendaciones de control interno que sean potencial factor de riesgo.
- d) Incluir en el Plan Operativo Anual de Auditoría Interna, las actividades de evaluación y control referidas a riesgos, los que deberán ser informados a la Máxima Autoridad Ejecutiva y al Directorio.

6.5.5 DE LAS UNIDADES DE LA ENTIDAD

- a) Identificar y comunicar Riesgos a la unidad de Riesgos, eventos de riesgos para su análisis.
- b) Apoyar a la Unidad de Riesgos en lo referente a recursos necesarios o ayuda para los procesos de auto evaluación en el que se identificarán los riesgos asociados a los procesos, productos, posición, entre otros que se lleven a cabo en sus respectivas áreas.

- c) Apoyar en el seguimiento de los indicadores referidos al riesgo establecidos por el Comité de Riesgos.
- d) Informe oportuno de eventos de pérdida por riesgos, así como su seguimiento.
- e) Informe oportuno de los eventos que afecten al logro de objetivos de la unidad, del área, institucionales, así como su seguimiento.
- f) Registrar las pérdidas ocasionadas por las categorías de riesgo de cada nivel de riesgos.
- g) Participar en las definiciones e implementación de acciones de control y mitigación del riesgo, definidas en el Plan de Manejo de Riesgos.

6.6 MARCO LEGAL Y TECNICO

6.6.1 Normativa Nacional

- Ley N° 1178, ley marco de los Sistemas de Administración Financiera y Control (SAFCO), que establece el control gubernamental como un sistema de gestión pública e integrado a los sistemas de planificación y administración.
- Principios, Normas Generales y Básicas de Control Gubernamental, aprobado el 21/09/2000 por la Ex Contraloría General de la República actualmente Contraloría General del Estado
- Guía para la aplicación de los principios, normas Generales y Básicas de Control Interno Gubernamental CI/10, documento de apoyo para la implantación de los Principios, Normas Generales y Básicas de Control Interno Gubernamental CI/08, fue aprobado el 31/10/2002 con resolución CGR-1/173/2002 y entra en vigencia a partir del 1/12/2002
- Guía para la implantación del Control Interno G/CE-21, documento de carácter normativo secundario de control para la implantación del Control Interno Gubernamental G/CE -21, fue aprobado el 23/10/2008 con resolución CGR-1/245/2008.

6.6.2 Normas técnicas internacionales

- COSO II – ERM el Marco de Control Interno Basado en Riesgos.
- INTOSAI GOV 9130, Administración de Riesgos de la Entidad de la INTOSAI
- Norma AS/NZS 4360:2004 de Administración de Riesgos.
- ISO 31000 Gestión de Riesgos

6.7 MARCO CONCEPTUAL

El propósito de la Administración Pública es la satisfacción de las necesidades de la sociedad en todo momento, para lo cual le corresponde establecer una planificación institucional, la organización y dirección, el seguimiento y evaluación, la ejecución de los recursos, conforme a la Ley 1178 para alcanzar los fines esenciales del Estado. Todo esto requiere legitimidad, eficacia en el servicio y que prime siempre el interés de la sociedad.

Bajo este contexto, la Administración Pública Boliviana debe considerar la creciente complejidad e incertidumbre de la realidad social y económica actual, que conllevan dinámicas de cambios, ya que muchas veces simultáneamente aparecen conceptos que requieren apropiación de conocimientos y tecnologías, a ser servicio público lo que prestan las Entidades Públicas Financieras no Bancarias se exige procesos concretos y precisa de productos y servicios que respondan a las necesidades y expectativas de sus clientes y comunicar a la sociedad de ello en el marco de las políticas de transparencia.

Para aproximar estas dinámicas de la realidad actual a la administración del sector público, en especial en las Entidades Públicas Financieras no Bancarias que administran recursos financieros líquidos, es necesario formalizar herramientas o metodologías que busquen minimizar la probabilidad de ocurrencia de riesgos en el cumplimiento de los objetivos asignados; e incluso se pueda pretender permanecer y no desaparecer por impactos negativos en la ejecución de la gestión, inclusive llevar a tomar la decisión gubernamental de desaparición de estas entidades públicas

Por ello es importante resaltar la trascendencia del concepto de riesgo en estas entidades del estado, ya que estos con la debida administración, se minimiza, reduce o elimina su impacto en el logro de la misión y objetivos encomendados.

¿Pero cuáles son los riesgos a los que están expuestos las Entidades Públicas Financieras no Bancarias?

Está expuesta a riesgos potenciales cuyas fuentes son determinadas por aspectos que están fuera de su control. Por Ejemplo: eventos naturales (terremotos, inundaciones), incendios, atentados, riesgos financieros, accidentes de trabajo, etc. Otros factores de carácter externo, denominados del entorno y que atentan contra su naturaleza jurídica y administrativa, como son los cambios producidos en la normativa, jurisprudenciales, presupuestales y cambios en políticas gubernamentales que en un momento determinado pueden llegar a incidir en el cumplimiento de su objeto social y competencias institucionales.

También están expuestas al deterioro de su imagen, como consecuencia de la opinión ciudadana, el control social y de los medios de comunicación en general, debido a que factores de riesgo no permiten poner en práctica planes y programas para hacer de este tipo de entidades eficaces en términos de generación de resultados, pero sobre todo, más comprometida con las verdaderas demandas, expectativas y necesidades de la sociedad y de sus clientes.

Por otro lado, existen factores de orden interno los cuales fueron identificados por las unidades con base en las funciones y actividades que ejecutan estos se destacan en : el manejo de los recursos, la estructura organizacional, los controles existentes, los procesos y procedimientos, la disponibilidad presupuestal, la forma de vinculo de los servidores públicos con la Entidad, los intereses de la alta dirección, el nivel del talento humano, la motivación y los niveles salariales, entre otros. A este conjunto de riesgos se los denomina riesgos absolutos, los que, una vez les son aplicados controles efectivos, reducen significativamente su consecuencia o impacto y probabilidad de ocurrencia.

Aunque no existe un método único que se pueda considerar un estándar, para evaluar el control y medir qué tanto mitiga el riesgo asociado, es importante establecer una serie de tratamientos para aplicar; uno de ellos se desarrolla mediante una serie de controles de tipo preventivo y correctivo traducidos en lineamientos, políticas y estrategias implementados a nivel interno. Para el caso de estas Entidades, estos han sido clasificados en generales y específicos; entre los primeros se encuentran aquellos dirigidos hacia la ejecución de la gestión Institucional, mientras que los segundos son específicos para la ejecución del proceso. También aquellos de origen externo, sobre los cuales se exige su cumplimiento.

Es indispensable contar con un plan de manejo de los riesgos para realizarles monitoreo permanente, teniendo en cuenta que estos nunca se eliminan. Se mitigan. Es más, pueden aparecer nuevas amenazas que hace necesario ajustarlos.

6.7.1 Factores de Riesgo

Los factores de riesgo, son aquellas fuentes generadoras de eventos que pueden originar pérdidas en las operaciones o afectar al logro de los objetivos generales o de los procesos. Corresponden entonces, a aquellos agentes cuya variación imprevista puede ocasionar resultados operativos adversos. Dichos factores pueden ser internos o externos a la organización.

Son factores internos de riesgo: los recursos humanos, los procesos, la tecnología y la infraestructura, sobre los cuales la organización puede tener un control directo.

Son factores externos de riesgo: los acontecimientos externos cuyas causas y origen escapan al control a la organización y pueden estar relacionados con fuerzas de la naturaleza o con actuaciones de terceros, por ejemplo, cambio en las normas legales o instauración de procesos jurídicos en contra de la institución y decisiones judiciales o administrativas adversas a la Entidad, incendios o atentados, convulsión social, etc.

El **RECURSO HUMANO**, está constituido por el conjunto de servidores públicos vinculados directa o indirectamente a la entidad en la ejecución de sus procesos.

Los **PROCESOS** son las interrelaciones de las actividades, que conllevan la transformación de elementos de entrada o insumos, a fin de obtener productos o servicios destinados a satisfacer necesidades de las personas que los demandan. Los procesos constituyen factor de riesgo, en tanto que las características de los productos pueden variar dependiendo del desarrollo de los procedimientos que se lleven a cabo para conseguirlos.

La **TECNOLOGÍA**, es el conjunto de instrumentos empleados para mejorar de una manera sistemática los procesos. Para el caso de las entidades públicas financieras no bancarias, los elementos de informática (software y hardware) y de telecomunicaciones, constituyen su principal soporte tecnológico, cuyas características implican un riesgo importante o material.

La **INFRAESTRUCTURA** corresponde a los elementos de apoyo diferentes a aquellos de carácter tecnológico como las instalaciones, los puestos de trabajo y los mecanismos de logística.

6.7.2 Mapa de procesos

La premisa principal para la administración de los riesgos operativos, se refiere a su enfoque hacia los procesos, en congruencia con uno de los principios de Gestión de la Calidad. Por lo tanto, es requisito indispensable para iniciar el desarrollo de dicha administración, disponer del MAPA DE PROCESOS institucional previamente definido y debidamente aprobado, incluyendo las respectivas interrelaciones y objetivos de cada proceso, en la Figura 20 se muestra un modelo de mapa de procesos claves tipo de una Entidad Pública Financiera no Bancaria.



Figura 20 Mapa de Procesos Claves

El esquema de procesos institucionales para efectos de administración del riesgo debe servir de referente y será el que se adopte formalmente por la Dirección General. En todo caso, las modificaciones que se introduzcan a dicho mapa de procesos, deberán estar soportadas por los análisis de riesgos pertinentes, elaborados con aplicación de los procedimientos contenidos en el presente manual.

6.8 METODOLOGIA

Las entidades públicas financieras no bancarias con el objeto de darle cumplimiento a su misión constitucional y competencia legal, a través de los objetivos estratégicos e institucionales los cuales se desarrollan a partir del diseño y ejecución de los diferentes planes, programas y proyectos. El cumplimiento de dichos objetivos puede verse afectado por la presencia de riesgos, ocasionados por factores tanto internos como externos, razón por la cual se hace necesario contar con acciones tendientes a administrarlos dentro de la entidad.

En el presente manual se establece el enfoque de gestión de riesgos a nivel estratégico y de procesos o actividades, es decir, identificar los riesgos para dos grupos, uno para factores de riesgo estratégico y otro para factores de riesgo implícitos en los procesos.

El adecuado manejo de los riesgos favorece al desarrollo y crecimiento de la entidad, con el fin de asegurar dicho manejo es importante que se establezca el entorno en el que se desenvuelve la entidad, el establecimiento del contexto, la identificación, análisis, valoración y definición de las alternativas de acciones de mitigación de los riesgos de acuerdo a lo siguiente:

Comparación de la metodología propuesta con la Guía G/CE-21 emitida por la contraloría General del Estado.

Etapas del proceso	Producto	Según Guía G/CE-21
Establecimiento del Contexto	 Mapa de Riesgos	No describe
Identificación de riesgos		Identificación de Eventos
Análisis de riesgos		Evaluación de Eventos
Valoración de riesgos		
Políticas de Administración de Riesgos	Plan de Manejo de los Riesgos	Respuesta a los riesgos
Monitoreo		No describe

DIRECTRICES GENERALES

Las fases fundamentales sugeridas para una adecuada Administración o Gestión del Riesgo Operativo son las siguientes:

Compromiso de la Máxima Autoridad Ejecutiva (MAE) y del Directorio: Para el éxito en la Implementación de una adecuada Administración del Riesgo, es indispensable el compromiso de la MAE como encargada, en primera instancia, de establecer el marco para la gestión del riesgos, en segunda instancia el de estimular la cultura del riesgo en sus etapas de la identificación y prevención del riesgo y en tercera instancia de definir las políticas. Para lograrlo es importante la definición de canales directos de comunicación y el apoyo a todas las acciones emprendidas en este sentido, propiciando los espacios y asignando los recursos necesarios. Así mismo, debe designar a un responsable de nivel jerárquico para que asesore y apoye todo el proceso de diseño e implementación del proceso de Gestión del Riesgo.

Conformación de un Equipo de Riesgo: Es importante conformar un equipo que se encargue de liderar el proceso de gestión del riesgo dentro de la entidad y cuente con un

canal directo de comunicación con el responsable designado por MAE y las personas designadas para trabajar el tema en las diferentes dependencias. Dicho equipo lo deben integrar personas de diferentes áreas que conozcan muy bien la entidad y el funcionamiento de los diferentes procesos para que se facilite la gestión del riesgo y la construcción de los mapas de riesgos institucionales.

Capacitación en gestión de riesgo y la metodología: Definido el Equipo de Riesgo, debe capacitarse a sus integrantes en la metodología de Gestión de Riesgo Operativo. Asimismo los gerentes o directores de área en la actualización de sus procesos operativos de cada área donde deben integrar a partir de las problemáticas de su entorno los factores de riesgo inherentes al desarrollo institucional y administrativo.

6.8.1 ESTABLECIMIENTO DEL CONTEXTO

Para la formulación y operativización del proceso de la gestión del riesgo es fundamental tener claridad de la misión institucional, sus objetivos estratégicos e institucionales y tener una visión sistémica de la gestión de manera que no se perciba esta herramienta gerencial como algo aislado del mismo accionar administrativo. Por ende, el diseño se establece a partir de la identificación de los factores internos o externos a la entidad que pueden generar riesgos que afecten el cumplimiento de sus objetivos.

Conforme a la Guía para la implantación del Control Interno G/CE-21 que establece para la implantación del Control Interno que es necesaria la evaluación de riesgos y por lo tanto establecen un procedimiento mínimo para el subcomponente de evaluación de riesgos como elemento de Control, sin embargo desde un enfoque de auditoría y control y no así como una herramienta de gestión que permita establecer el lineamiento estratégico que orienta las decisiones de la entidad pública, frente a los riesgos que pueden afectar el cumplimiento de sus objetivos producto de la observación, distinción y análisis del conjunto de circunstancias internas y externas que puedan generar eventos que originen oportunidades o afecten el cumplimiento de su competencia, misión y objetivos institucionales”.

El Establecimiento del Contexto es la base para la identificación de los riesgos que afecten a los objetivos estratégicos y a los procesos sustantivos y de soporte conforme al mapa de procesos institucional, el análisis se realiza a partir del conocimiento de situaciones del entorno de la entidad, tanto de carácter social, económico, cultural, de orden público, político, legal y /o cambios tecnológicos, entre otros; se alimenta también con el análisis de la situación actual de la entidad, puede obtener información de los resultados de la evaluación del Ambiente de Control, Estructura Organizacional, Modelo de Operación, cumplimiento de los Planes y Programas, sistemas de información, procesos y procedimientos y presupuesto institucional, entre otros.

Se recomienda la aplicación de varias herramientas y técnicas como por ejemplo: entrevistas estructuradas con expertos en el área de interés, reuniones con directores y con personas de todos los niveles en la entidad, evaluaciones individuales usando cuestionarios, lluvias de ideas con los servidores públicos de la entidad, entrevistas e indagaciones con personas ajenas a la entidad, usar diagramas de flujo, análisis de escenarios y hacer revisiones periódicas de factores económicos y tecnológicos que puedan afectar la organización, entre otros. Igualmente pueden utilizarse diferentes fuentes de información de la entidad, tales como registros históricos, experiencias significativas registradas, opiniones de especialistas y expertos, informes de auditoría y consultoría de años anteriores, los cuales pueden proporcionar información importante, la técnica utilizada dependerá de las necesidades y naturaleza de la entidad.

Con la realización de esta etapa se busca que la entidad obtenga los siguientes resultados:

- Identificar los factores externos que pueden ocasionar la presencia de riesgos, con base en el análisis de la información externa y los planes, programas y proyectos de la entidad.
- Identificar los factores internos que pueden ocasionar la presencia de riesgos con base en el análisis de los componentes Ambiente de Control, Direccionamiento

Estratégico y demás estudios que sobre la cultura organizacional y el clima laboral que se hayan adelantado en la entidad.

- Aportar información que facilite y enriquezca las demás etapas del proceso de la gestión de riesgos.

6.8.2 IDENTIFICACIÓN DE RIESGOS

El proceso de la identificación del riesgo debe ser permanente e interactivo basado en el resultado del Establecimiento del Contexto, en el proceso de planeación y debe partir de la claridad de los objetivos estratégicos de la entidad para la obtención de resultados, sin embargo adicionalmente debe identificarse riesgos en los procesos sustantivos de la entidad y los más riesgos más importantes en los procesos de soporte o apoyo de acuerdo al mapa de procesos establecido en el Establecimiento del Contexto.

Conforme a la Guía para la implantación del Control Interno G/CE-21 es un elemento de Control, que posibilita conocer los eventos potenciales, estén o no bajo el control de la Entidad Pública, que ponen en riesgo el logro de su Misión y objetivos, estableciendo los factores de riesgo, las causas y los efectos de su ocurrencia.

De acuerdo con el enfoque, la identificación de los riesgos se realiza a nivel Estratégico, identificando los factores internos o externos a la entidad, que pueden ocasionar riesgos que afecten el logro de los objetivos. Es la base del análisis de riesgos que permite avanzar hacia una adecuada implementación de políticas que conduzcan a su control.

Una manera para que todos los servidores de la entidad conozcan y visualicen los riesgos, es a través de la utilización del formato de identificación de riesgos el cual permite hacer un inventario de los mismos, definiendo en primera instancia las causas o factores de riesgo, tanto internos como externos, los riesgos, presentando una descripción de cada uno de estos y finalmente definiendo los posibles efectos.

Por otro lado, es importante centrarse en los riesgos más significativos para la entidad relacionados con el desarrollo de los procesos y los objetivos institucionales. Es allí donde, al igual que todos los servidores y la gerencia pública adopta un papel proactivo

en el sentido de visualizar durante la etapa del establecimiento del contexto y objetivos institucionales los factores o eventos que pueden afectar la dirección institucional, dada la especialidad temática que manejan en cada sector o contexto socioeconómico.

Entender la importancia del manejo del riesgo implica conocer con más detalle los siguientes conceptos:

- **Proceso:** Nombre del proceso
- **Objetivo del proceso:** se debe transcribir el objetivo que se ha definido para el proceso al cual se le están identificando los riesgos.
- **Factor:** ¿Cuáles son las variables internas y externas relacionadas con los objetivos de la entidad? Son aspectos internos y externos que contienen a las fuentes generadoras de eventos; por ejemplo: factores externos políticos, tecnológicos, sociales, etc.; y factores internos relacionados con la infraestructura, el personal, los procesos, etc.
- **Fuente de riesgo:** ¿Cuál es la fuente de cada riesgo? Representa algo que tiene potencial intrínseco para dañar o ayudar a ello (potencial de amenaza); por ejemplo, un producto combustible, la energía eléctrica, las recaudaciones, las contrataciones, los activos valiosos, el volumen de operaciones; la complejidad de las operaciones; presiones económicas, disconformidad del personal, desorganización, burocracia, ubicación de la entidad en zonas de riesgo ambiental, etc.
- **Evento o suceso:** ¿Qué puede o podría suceder? Es un incidente u ocurrencia, de fuentes internas o externas de la entidad que pueden o podrían afectar positiva o negativamente la implementación de la estrategia o el logro de objetivos; por ejemplo: errores, robos, hurtos, irregularidades, nuevas regulaciones o actualizaciones, etc.
- **Consecuencias:** ¿Cuál es el resultado o impacto sobre los objetivos? Son los efectos que genera el evento sobre los interesados y activos; por ejemplo: daños medioambientales, pérdidas financieras, pérdidas de bienes, ineficacias, ineficiencias, incumplimientos normativos, etc.

- **Causas:** ¿Qué y por qué puede ocurrir?; Son los motivos o razones para la presencia del riesgo o el evento que ocurre; por ejemplo: falta de supervisión, falta de medidas de seguridad, falta de capacidad técnica, etc.
- **Momento:** ¿Cuándo puede ocurrir?; Es la oportunidad en la que puede ocurrir el evento; por ejemplo, durante el fin de semana; en horario de trabajo, en el ingreso al almacén, etc.
- **Lugar:** ¿Dónde: puede ocurrir?; Es el espacio o circunstancia en la cual puede ocurrir el evento; por ejemplo: en el centro de cómputos, en la departamental de La Paz, en el almacén, en el archivo central, etc.

La identificación de eventos siempre parte de la determinación de los objetivos de la entidad, del área, de la unidad organizacional, del proceso o del procedimiento objeto de análisis.

Sobre la base de los objetivos se desarrollan las técnicas predeterminadas considerando los factores relacionados:

Factores Externos

▪ **Económicos**

Los eventos relacionados pueden incluir atrasos en las transferencias, no obtención de financiamiento externo, recortes presupuestarios, cambios en el tipo de cambio, etc.

▪ **Condiciones ambientales**

Los eventos relacionados pueden incluir incendios, inundaciones, sismos, etc.

▪ **Políticos**

Los eventos relacionados pueden incluir cambios gubernamentales, cambios en las leyes, decretos y otras normas de regulación, cambios en las agendas políticas, etc.

▪ **Sociales**

Los eventos relacionados pueden incluir cambios demográficos por emigración o inmigración, nuevas demandas sociales, demandas insatisfechas, etc.

▪ **Tecnológicos**

Los eventos relacionados pueden incluir exigencias para migrar antiguos sistemas a las nuevas tecnologías, escasez de insumos para el hardware existente en la entidad, etc.

▪ **Relacionamiento con Sujetos de Financiamiento**

Los eventos relacionados con la comunicación con nuestros clientes pueden generar documentación insuficiente durante el proceso de financiamiento que repercute en el proceso de colocación de préstamos desde la evaluación hasta la ejecución.

Factores Internos

▪ **Infraestructura**

Los eventos relacionados pueden incluir reparaciones inesperadas, superpoblación de instalaciones, equipos insuficientes para las demandas internas y/o externas, etc.

▪ **Personal**

Los eventos relacionados pueden incluir incremento de accidentes, incremento de errores humanos, irregularidades por fraudes, retiro de personal experimentado, etc.

▪ **Procesos**

Los eventos relacionados pueden incluir deficiencias en los productos y servicios, retrasos en la prestación de servicios, retrasos en las contrataciones, etc.

▪ **Tecnología**

Los eventos relacionados pueden incluir computadoras necesarias fuera de servicio, pérdida de información procesada, pérdida de confidencialidad de la información; errores en las salidas de la información procesada; etc.

Se debe considerar que la causa no siempre es única al igual que las consecuencias. En este sentido, es conveniente que se incluyan las posibles causas y consecuencias para un mayor análisis posterior en la etapa de análisis de riesgos. Adicionalmente, es conveniente que el evento manifieste el momento y el lugar donde puede o podría ocurrir, cuando corresponda.

MATRIZ DE IDENTIFICACION DE EVENTOS									
PROCESO	OBJETIVO	FACTOR	FUENTE	EVENTO DE RIESGO	CONTROLES	CAUSAS	CONSECUENCIAS	MOMENTO	LUGAR
Estrategico	Ejecutar 20 MM de US\$	Relacionamiento con Sujetos	Comunicación	Presentación inoportuna de documentos de los sujetos de financiamiento.	Se cuenta con un Reglamento Operativo.	Alta rotación de personal técnico en los sujetos de financiamiento.	Disminución de la cartera de prestamos	Fin de mes	Oficina Central
Recuperación	Recuperar los prestamos realizados en forma oportuna, confiable y eficiente.	Personal	Calculos Manuales	Error en la determinación de la tasa de interes	No se han diseñado controles.	Desconocimiento del origen de la información para determinar la tasa.	Cobro de intereses con error por subvaluación.	Semestralmente	Gerencia de Finanzas
Contabilidad	Conciliar saldos de cartera y aporte local.	Personal	Errores Contables	Los saldos contables no concilien con los clientes.	Existe un procedimiento de conciliación	Desconocimiento del procedimiento de conciliación.	Saldos de cartera y aporte local no confiables.	Mensual.	Unidad de Contabilidad

Clasificación del riesgo

Durante el proceso de identificación del riesgo se recomienda clasificarlos teniendo en cuenta los siguientes conceptos, mínimos pudiendo ser aumentados según la entidad:

Riesgo Estratégico: Se asocia con la forma de la administración estratégica de la entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

Riesgos Operacionales: Comprende los riesgos relacionados tanto con la parte operativa como con la técnica de la entidad, incluye riesgos provenientes de deficiencias en los sistemas de información, en la definición de los procesos operativos, en la estructura de la entidad, la falta de coordinación y comunicación entre unidades, lo cual conduce a ineficiencias, oportunidades de corrupción e incumplimiento de los compromisos institucionales.

Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad, que incluye la ejecución presupuestal, determinación de tasas de interés, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes de cada entidad. De la eficiencia y transparencia en el manejo de los recursos, así como de su interacción con las demás áreas, dependerá en gran parte el éxito o fracaso de toda entidad.

Riesgos de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad, por ejemplo remisión de contratos a la CGE, rendición de cuentas pública, etc.

Riesgos de Tecnología: Se asocian con la capacidad de la entidad para que la tecnología disponible satisfaga sus necesidades actuales y futuras y soporte el cumplimiento de la misión.

FUENTES DEL RIESGO	PROCESO EN EL QUE IMPACTA				
	Proceso 1	Proceso 2	Proceso 3	Proceso 4	Proceso 5
Estratégico					
Operativo					
Financiero					
Cumplimiento					
Tecnología					

La anterior tabla muestra cómo se asocia la Identificación del Riesgo a los procesos de la entidad; también es posible adaptar la tabla a las actividades de los procesos cuando se trata del proceso de Administración del Riesgo por Procesos.

Con la realización de esta etapa se busca que la entidad obtenga los siguientes resultados:

- Determinar las causas (factores internos o externos) de las situaciones identificadas como riesgos para la entidad.
- Describir los riesgos identificados con sus características.
- Precisar los efectos que los riesgos puedan ocasionar a la entidad

6.8.3 EVALUACIÓN DE RIESGOS (ANÁLISIS DE RIESGOS)

La Evaluación de Riesgos busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos, con el fin de obtener información para establecer el nivel de riesgo. La primera representa el número de veces

que el riesgo se ha presentado en un determinado tiempo o puede presentarse, y la segunda se refiere a la magnitud de sus efectos.

La Evaluación del riesgo dependerá de la información obtenida en el formato de identificación de riesgos y de la disponibilidad de datos históricos y aportes de los servidores de la entidad. Los riesgos identificados son evaluados para establecer una base y determinar como deben ser administrados, estos se asocian con los objetivos y procesos que pueden verse afectados y son evaluados sobre una doble perspectiva inherente y residual. Con el objeto de comprender el perfil de riesgo y la jerarquía del riesgo para establecer los planes de acción en función a la importancia del riesgo.

6.8.3.1 Calificación del Riesgo

Se logra a través de la estimación de la **Frecuencia de Ocurrencia (FO)** y la **Importancia del Riesgo (IR)** del impacto que puede causar la materialización del riesgo. Para establecer estos criterios de valoración de riesgos la entidad debe contar con escalas de valores determinados por importancia del riesgo de las consecuencias, frecuencia de ocurrencia y probabilidades.

Frecuencia de Ocurrencia (FO): La escala para determinar este indicador habitualmente tienen un mínimo de tres niveles aunque existen escalas más complejas de cuatro, cinco y seis niveles para considerar el impacto de los eventos y su probabilidad de ocurrencia.

Las escalas de valores de las consecuencias y probabilidades deben ser elaboradas por la unidad responsable de Gestión de Riesgos, es necesario establecer las escalas de medición y niveles, así como el significado de cada nivel. Generalmente, para temas administrativos y operativos se utilizan escalas de tres niveles que son fácilmente comprendidas debido a la sencillez de sus conceptos.

Para elaborar las escalas se deben realizar, al menos, las siguientes tareas:

- Establecer los niveles junto a la definición y descripción de cada uno de ellos para los impactos o consecuencias de los eventos.
- Establecer los niveles junto a la definición y descripción de cada uno de ellos para las probabilidades de ocurrencia de los eventos.
- Definir el horizonte del tiempo al cual se refiere la escala de probabilidades de ocurrencia y los criterios aplicables.
- Definir los criterios a considerar para establecer los niveles de las magnitudes de los eventos.

Con relación al horizonte de tiempo para definir si un evento ocurre o podría ocurrir con mayor o menor frecuencia o probabilidad, se debe considerar 1 año a efectos de la identificación de eventos relacionados con los objetivos institucionales y de gestión de las unidades organizacionales. Para los eventos relacionados con los objetivos estratégicos se debe tomar en cuenta la duración del período estratégico, por ejemplo 5 años.

Respecto de la identificación de eventos a nivel de procesos y procedimientos, es conveniente considerar los siguientes criterios:

- La cantidad de veces que el procedimiento se desarrolla dentro de una gestión y si el evento puede ocurrir en todos los procedimientos, o en algunos; y
- La cantidad de veces que el evento ocurre en cada procedimiento; siendo factible que ocurra una vez o en varias oportunidades; o nunca.

A manera de ejemplo se presentan las siguientes escalas aplicables para la Frecuencia de Ocurrencia (FO):

TABLA DE DETERMINACION RECURRENCIA O FRECUENCIA

Probabilidad de Recurrencia o Frecuencia			
Nivel	Calificación	Grado Tiempos	Característica
Probable	Muy Común	1 vez a la semana	Se espera que ocurra en la mayoría de las circunstancias
Probable	Común	1 vez al mes	Probablemente ocurrirá en la mayoría de las circunstancias o en algún
Posible	Frecuente	1 vez al trimestre	

			momento
Posible	Ocasional	1 vez cada semestre	Pudo ocurrir en algún momento
Remoto	Raro	Menos de 1 vez al año	Puede ocurrir solo en circunstancias excepcionales.

El cual puede quedar resumido en el siguiente cuadro:

Nivel	Definición	Descripción
1	Remoto	El evento es infrecuente o se presume que no podría ocurrir.
2	Posible	El evento ocurre frecuentemente o se presume que posiblemente ocurrirá.
3	Probable	El evento ocurre muy frecuentemente o se presume que seguramente ocurrirá.

Importancia del Riesgo (IR): Para esta clasificación se deben considerar, al menos, los siguientes criterios:

Objetivos relacionados con el cumplimiento de leyes y normas:

- Consecuencias penales y su relación con los intereses del estado y la sociedad.
- Consecuencias civiles y su relación con los intereses del estado y la sociedad.
- Consecuencias administrativas y su relación con los intereses del estado y la sociedad.

También deben considerar los intereses del directorio cuando corresponda y la máxima autoridad ejecutiva respecto del cumplimiento de leyes y normas independientemente de los posibles montos relacionados con los eventos.

Objetivos relacionados con la confiabilidad de la información financiera:

- Valor estimado de la consecuencia sobre el valor de los activos totales.
- Valor estimado de la consecuencia sobre el valor del patrimonio.
- Valor estimado de la consecuencia sobre el valor de los ingresos.
- Valor estimado de la consecuencia sobre el valor de los gastos.

Objetivos relacionados con la eficacia y eficiencia operativa:

- Consecuencia sobre el objetivo del proceso o procedimiento
- Consecuencia sobre el valor de los almacenes al cierre de un período determinado.
- Consecuencia sobre el valor de los activos fijos al cierre de un período determinado.
- Consecuencia sobre el valor del dinero disponible en un período determinado

Objetivos relacionados con la planificación estratégica y operativa:

- Consecuencia sobre el objetivo estratégico relacionado.
- Consecuencia sobre el objetivo institucional relacionado.
- Consecuencia sobre el objetivo de gestión del área o unidad organizacional.
- Consecuencia sobre las operaciones programadas del área o unidad organizacional

Asimismo, se deben considerar los perjuicios que se pueden generar en la imagen de la institución y las prioridades que hayan establecidos los ejecutivos en relación con la eficacia y eficiencia de las operaciones independientemente de los posibles montos relacionados.

No obstante, para los objetivos operacionales es indispensable que la entidad haya definido la “Tolerancia al Riesgo” que constituye el desvío aceptable en el logro de los objetivos. La tolerancia al riesgo representa el marco dentro del cual se valorarán las consecuencias de los eventos operacionales.

La estimación de la importancia del riesgo por el impacto posible que generará la ocurrencia del evento podrá ser estimada en una primera etapa de forma cualitativa a través de un análisis subjetivo.

En ella se utilizará el método de simulación de escenarios (método cualitativo), el cual medirá el impacto de acuerdo a una descripción de escenarios calificados previamente, como el siguiente:

**TABLA DE MEDICION DEL IMPACTO Y LA IMPORTANCIA DEL
RIESGO**

Categoría	Grado	Característica
Muy Significativo	Catastrófico 2	Riesgo de continuidad del negocio, destrucción de infraestructura, información, documentos y/o ingresos
	Catastrófico 1	Riesgo de exposición significativa a quejas importantes por incumplimiento de contratos y normas legales.
Significativo 2	Importante 2	Riesgo de interrupción de una parte de las operaciones de procesos claves.
	Importante 1	Riesgo de alteración o corrupción de datos y

		transferencia de datos.
Significativo 1	Moderado 3	Riesgo de pérdida de oportunidades de recursos
	Moderado 2	Riesgo de infracciones a la regulación o normativa.
	Moderado 1	Riesgo de demoras significativas en operaciones.
Poco significativo	Menor 2	Riesgo de reducción de ingresos no significativos
	Menor 1	Riesgo en procesos rutinarios no importantes
	Muy poco significativo 2	Riesgo de demoras en las actividades administrativas de apoyo sin importancia.
	Muy poco significativo 1	Riesgo de inconvenientes menores.

El cual puede quedar resumido en la siguiente escala aplicable:

Nivel	Definición	Descripción
1	Poco significativo	La consecuencia del evento no afectará el logro del objetivo relacionado.
2	Significativo	La consecuencia del evento afectará pero no impedirá el logro del objetivo relacionado.
3	Muy significativo	La consecuencia del evento impedirá el logro del objetivo relacionado.

6.8.3.2 Evaluación del Riesgo

Permite comparar los resultados de la calificación de los riesgos con los criterios definidos para establecer el grado de exposición de la entidad al riesgo (Nivel de riesgo); de esta forma es posible distinguir entre los riesgos aceptables, tolerables, moderados, importantes o inaceptables y fijar las prioridades de las acciones requeridas para su tratamiento.

La metodología para determinar el nivel de riesgos debe ser elaborada por la unidad responsable de Gestión de Riesgos, sin embargo, Cuantitativamente la evaluación del riesgo es el producto automático, realizado mediante una formula matemática que resulta de la relación entre la Frecuencia de Ocurrencia y el impacto del riesgo evaluado.

No obstante, la valoración debe ser efectuada por los responsables de las áreas y unidades organizacionales que han identificado sus eventos aplicando los criterios preestablecidos y utilizando las escalas disponibles.

Las áreas y unidades deben respaldar sus valoraciones sobre consecuencias y probabilidades para las revisiones que considere necesarias el Comité de Gestión de Riesgos y la unidad encargada de la Gestión de Riesgos.

La representación de la cuantificación obtenida en la matriz o grafico, que permite la observación del resultado de la evaluación del riesgo identificado, esta información podrá ser registrada en el formato siguiente:

MATRIZ DE EVALUACION DEL RIESGO											
ID	PROCESO	OBJETIVO	FACTOR	FUENTE	EVENTO DE RIESGO	CONSECUENCIAS	IMPACTO		PROBABILIDAD		EVALUACION DEL RIESGO
							NIVEL	VALOR	NIVEL	VALOR	
E-01	Estrategico	Ejecutar 20 MM de US\$	Relacionamiento con Sujetos	Estrategico	Presentación inoportuna de documentos de los sujetos de financiamiento.	Disminución de la cartera de prestamos	Medio	2	Medio	2	4
F-01	Recuperación	Recuperar los prestamos realizados en forma oportuna, confiable y eficiente.	Personal	Financiero	Error en la determinación de la tasa de interes	Cobro de intereses con error por subvaluación.	Alto	3	Medio	2	6
F-02	Contabilidad	Conciliar saldos de cartera y aporte local.	Personal	Financiero	Los saldos contables no concilien con los clientes.	Salos de cartera y aporte local no confiables.	Medio	2	Bajo	1	2
O-01	Administración	Seguro de Bienes y cauciones	Infraestructura	Operativo	Incendio	Destrucción de infraestructura institucional y documentación.	Alto	3	Bajo	1	3

Conforme a la metodología se adiciona la siguiente información luego de la identificación y en función a la calificación que se obtiene asignándoles un valor para el impacto o Importancia Relativa y la probabilidad o Frecuencia de Ocurrencia.

- **Impacto o Importancia del Riesgo (IR):** el valor numérico asignado en función a la calificación.
- **Probabilidad o Frecuencia de Ocurrencia(FO):** el valor numérico asignado en función a la calificación.
- **Evaluación del Riesgo:** que es el resultado de la multiplicación del impacto por la probabilidad

6.8.3.3 Determinación del nivel del riesgo (Valoración del Riesgo)

La determinación del nivel de riesgo es el resultado de confrontar el impacto y la probabilidad (evaluación del riesgo obtenida) con los controles existentes en los

diferentes procesos y procedimientos que se realizan. Para adelantar esta etapa se deben tener muy claros los puntos de control existentes en los diferentes procesos, los cuales permiten obtener información para efectos de tomar decisiones, estos niveles de riesgo pueden ser:

ALTO: Cuando el riesgo hace altamente vulnerable a la entidad o unidad. (IR y FO alta vs controles)

MEDIO: Cuando el riesgo presenta una vulnerabilidad media. (IR alto - FO baja o IR bajo – FO alta vs controles).

BAJO: Cuando el riesgo presenta vulnerabilidad baja. (IR y FO baja vs controles).

Calificación de los controles:

Para la evaluación de los controles existentes de cada uno de los riesgos, es necesario establecer si son preventivos o correctivos y responder las siguientes preguntas:

¿Están documentados?

¿Se están aplicando en la actualidad?

¿Son efectivos en minimizar el riesgo?

Criterios para evaluar el nivel del riesgo

- Cuando la evaluación de los controles es alta, disminuye el nivel del riesgo.
- Cuando la evaluación de los controles existentes es media:
 - ✓ Si la evaluación de riesgo es media, el nivel de riesgo pudiera mantenerse en medio si su referencia marcadora es la probabilidad (probabilidad alta impacto bajo);
 - ✓ Si su referencia marcadora es el impacto (impacto alto probabilidad baja) el nivel del riesgo pudiera aumentar a alto.
- Cuando la evaluación de los controles existentes baja, aumenta el nivel de riesgo o mantiene si esta relacionado con la probabilidad.

Siguiendo con la elaboración del formato y partiendo de la evaluación del Riesgo obtenido, se incluye lo relativo a la evaluación de controles existentes, la identificación

del control, si el mismo existe, si está documentado, si se aplica, si es efectivo, y la correspondiente evaluación del control de acuerdo a la aplicación de los criterios para evaluar la efectividad de los controles existentes, finalmente la valoración del Riesgo de acuerdo a los criterios desarrollados para evaluar el nivel del riesgo de acuerdo a la siguiente tabla:

CRITERIOS	VALORACION DEL RIESGO
No existen Controles	Se mantiene o incrementa el resultado de la evaluación de antes de controles.
Los controles existentes no son efectivos	Se mantiene el resultado de la evaluación antes de controles.
Los controles existentes son efectivos pero no están documentados	Cambia el resultado a una casilla inferior de la matriz de evaluación antes de controles (el desplazamiento depende de sí el control afecta el impacto o la probabilidad)
Los controles son efectivos y están documentados.	Pasa a escala inferior (el desplazamiento depende de si el control afecta el impacto o la probabilidad)

Un ejemplo de la determinación del nivel del riesgo y del grado de exposición al mismo:

Riesgo: Pérdida de información debido a la entrada de un virus en la red de información de la entidad.

Probabilidad (FO): Alta, porque todos los computadores de la entidad están conectados a la red de Internet e intranet.

Impacto (IR): Alto, porque la pérdida de información traería consecuencias graves para el que hacer de la entidad.

Controles existentes: La entidad tiene establecidos controles semanales haciendo Backups o copias de seguridad y vacunando todos los programas y equipos; además guarda la información más relevante desconectada de la red en un centro de información.

Resultado Nivel de riesgo:

Por lo tanto el nivel de riesgo es Medio por los controles establecidos.

Lo anterior significa que a pesar de que la probabilidad y el impacto son altos confrontado con los controles, se puede afirmar que el nivel de riesgo es medio y por lo tanto las acciones que se implementen entrarán a reforzar los controles existentes y a valorar la efectividad de los mismos.

MATRIZ DE VALORACION DEL RIESGO														
ID	PROCESO	OBJETIVO	FACTOR	FUENTE	EVENTO DE RIESGO	CONSECUENCIAS	IMPACTO		PROBABILIDAD		EVALUACION DEL RIESGO	CONTROLES	CAUSAS	VALORACION
							NIVEL	VALOR	NIVEL	VALOR				
E-01	Estrategico	Ejecutar 20 MM de US\$	Relacionamiento con Sujetos	Estrategico	Presentación inoportuna de documentos de los sujetos de financiamiento.	Disminución de la cartera de prestamos	Medio	2	Medio	2	4	Se cuenta con un Reglamento Operativo.	Alta rotación de personal técnico en los sujetos de financiamiento.	4
F-01	Recuperación	Recuperar los prestamos realizados en forma oportuna, confiable y eficiente.	Personal	Financiero	Error en la determinación de la tasa de interes	Cobro de intereses con error por subvaluación.	Alto	3	Medio	2	6	No se han diseñado controles.	Desconocimiento del origen de la información para determinar la tasa.	6
F-02	Contabilidad	Conciliar saldos de cartera y aporte local.	Personal	Financiero	Los saldos contables no concilien con los clientes.	Saldos de cartera y aporte local no confiables.	Medio	2	Bajo	1	2	Existe un procedimiento de conciliación	Desconocimiento del procedimiento de conciliación.	2
O-01	Administración	Seguro de Bienes y cauciones	Infraestructura	Operativo	Incendio	Destrucción de infraestructura institucional y documentación.	Alto	3	Bajo	1	3	Extintores, en cada piso, sistemas antiincendios, camaras	Climatológicas o fuentes externas, descuido del personal, etc.	3

Conforme a la metodología se adiciona la siguiente información luego de la evaluación de riesgos para determinar la valoración del riesgo.

- **Controles y su nivel de efectividad:** ¿Qué controles existen para el tratamiento del riesgo?
- **Causas:** se refiere a las causas que el control no tenga el efecto deseado sobre el riesgo? Son las actividades diseñadas para prevenir, detectar o corregir; por ejemplo: sistemas de detección, políticas, seguridad, entrenamiento, etc.
- **Valoración del Riesgo:** Finalmente la valoración final del riesgo una vez evaluado los controles.

Con la realización de esta etapa se busca que la entidad obtenga los siguientes resultados:

- Identificación de los controles existentes para los riesgos identificados y analizados.
- Priorización de los riesgos de acuerdo con los resultados obtenidos de confrontar la evaluación del riesgo con los controles existentes, a fin de establecer aquellos que pueden causar mayor impacto a la entidad en caso de materializarse.

- Elaborar el mapa de riesgos para cada proceso.

6.8.4 POLÍTICAS DE ADMINISTRACION DE RIESGOS

Para determinar las Políticas de Administración de Riesgos se deben tener en cuenta todas las etapas anteriormente desarrolladas en el ejercicio de la administración del riesgo.

Tiene que convertirse en un elemento de control, que permite estructurar criterios orientadores en la toma de decisiones, respecto al tratamiento de los riesgos y sus efectos al interior de la entidad.

Las políticas identifican las opciones para tratar y manejar los riesgos basadas en la Administración del Riesgo, a su vez transmiten la posición de la dirección y establecen las guías de acción necesarias a todos los servidores de la entidad.

Se deben tener en cuenta alguna de las siguientes opciones, las cuales pueden considerarse cada una de ellas independientemente, interrelacionadas o en conjunto.

- **Evitar el riesgo**, tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Un ejemplo de esto puede ser el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.
- **Reducir el riesgo**, implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles.

- **Compartir o Transferir el riesgo**, reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Es así como por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar.
- **Asumir un riesgo**, luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

Para el manejo de los riesgos se deben analizar las posibles acciones a emprender, las cuales deben ser factibles y efectivas, tales como: la implementación de las políticas, definición de estándares, optimización de procesos y procedimientos y cambios físicos entre otros. La selección de las acciones más conveniente debe considerar la viabilidad jurídica, técnica, institucional, financiera y económica y se puede realizar con base en los siguientes criterios:

- a) La valoración del riesgo,
- b) El balance entre el costo de la implementación de cada acción contra el beneficio de la misma.

Para la ejecución de las acciones, se deben identificar las áreas o responsables de llevarlas a cabo, definir un cronograma y unos indicadores que permitan verificar el cumplimiento para tomar medidas correctivas cuando sea necesario.

Con la realización de esta etapa se busca encauzar el accionar de la entidad hacia el uso eficiente de los recursos, la continuidad en la prestación de los servicios, la protección de los bienes utilizados para servir a la comunidad. Igualmente, se busca que la entidad tenga claridad sobre las políticas de Administración del Riesgo, las acciones de manejo de riesgo y el compromiso de la Dirección y de los servidores de la entidad.

6.8.4.1 Elaboración del Mapa de Riesgos por proceso y el institucional

El mapa de riesgos contiene a nivel estratégico los mayores riesgos a los cuales está expuesta la entidad, permitiendo conocer las políticas inmediatas de respuesta ante ellos tendientes a evitar, reducir, dispersar o transferir el riesgo; o asumir el riesgo residual, y la aplicación de acciones, así como los responsables, el cronograma y los indicadores.

Para el efecto se debe elaborar una matriz del mapa de riesgos por cada proceso para facilitar la administración del riesgo, el cual debe elaborarse al finalizar la etapa de Valoración del Riesgo.

6.8.4.2 Descripción del Mapa de riesgos

Conforme a la metodología este documento tiene que contener la siguiente información:

Evento de Riesgo: posibilidad de ocurrencia de un evento que pueda entorpecer el normal desarrollo de las funciones de la entidad y le impidan el logro de sus objetivos.

Impacto o Importancia del Riesgo (IR): consecuencias que puede ocasionar a la organización la materialización del riesgo.

Probabilidad o Frecuencia de Ocurrencia (FO): entendida como la posibilidad de ocurrencia del riesgo; ésta puede ser medida con criterios de Frecuencia, si se ha materializado (por ejemplo: No. de veces en un tiempo determinado), o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado.

Evaluación del riesgo: Resultado obtenido en la matriz de calificación, evaluación y

MATRIZ DE MAPA DE RIESGOS															
ID	PROCESO	EVENTO DE RIESGO	IMPACTO		PROBABILIDAD		EVALUACION DEL RIESGO	CONTROLES EXISTENTES	VALORACION DEL RIESGO	OPCIONES DE MANEJO	ACCIONES	RESPONSABLES	CRONOGRAMA		INDICADORES
			NIVEL	VALOR	NIVEL	VALOR							Fecha Inicio	Fecha Final	
E-01	Estrategico	Presentación inoportuna de documentos de los sujetos de financiamiento.	Medio	2	Medio	2	4	Se cuenta con un Reglamento Operativo.	4	Reducir	Mayor Socialización y capacitación de nuestros procesos a nuestros clientes	Unidad de Transparencia y atención al cliente	01/01/2013	30/06/2013	Cientes socializados y capacitados con actas
F-01	Recuperación	Error en la determinación de la tasa de interes	Alto	3	Medio	2	6	No se han diseñado controles.	6	Reducir	El sistema debe emitir la información para determinar la tasa	Unidad de Líneas Financieras y Cartera	01/01/2013	31/12/2013	Reportes de datos para determinar la tasa de interes
F-02	Contabilidad	Los saldos contables no concilien con los clientes.	Medio	2	Bajo	1	2	Existe un procedimiento de conciliación	2	Reducir	Revisar, capacitar y socializar sobre el uso del procedimiento.	Unidad de Contabilidad	01/01/2013	30/03/2013	Actas de capacitación y socialización
O-01	Administración	Incendio	Alto	3	Bajo	1	3	Extintores, en cada piso, sistemas antiincendios, camaras	3	Transferir	Contratar a una empresa aseguradora, coordinar con el GAM la tala de arboles viejos.	Unidad de Administración	01/01/2013	28/02/2013	Empresa contratada y notas enviadas al GAM.

respuesta a los riesgos.

Controles existentes: especificar cuál es el control que la entidad tiene implementado para combatir, minimizar o prevenir el riesgo.

Valoración del riesgo: es el resultado de determinar la exposición de la entidad al riesgo, luego de confrontar la evaluación del riesgo con los controles existentes.

Opciones de manejo: opciones de respuesta ante los riesgos tendientes a evitar, reducir, dispersar o transferir el riesgo; o asumir el riesgo residual

Acciones: es la aplicación concreta de las opciones de manejo del riesgo que entrarán a prevenir o a reducir el riesgo y harán parte del plan de manejo del riesgo.

Responsables: son las dependencias o áreas encargadas de adelantar las acciones propuestas.

Cronograma: son las fechas establecidas para implementar las acciones por parte del grupo de trabajo.

Indicadores: se consignan los indicadores diseñados para evaluar el desarrollo de las acciones implementadas.

6.8.4.3 Priorización de los riesgos

Una vez realizado el análisis de los riesgos con base en los aspectos de probabilidad e impacto, se recomienda utilizar la matriz de priorización que permite determinar cuales requieren de un tratamiento inmediato.

Esta matriz se realiza en primera instancia al interior de cada un de los procesos, los resultados que de aquí se deriven servirán para socializarlos con el comité de riesgos y las áreas afectadas.

De esta manera existirán tantas matrices de priorización como procesos existan en la institución.

MATRIZ DE CALIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS

Probabilidad	Valor					
Probable	3	3 A Zona de Riesgo Moderado Evitar el Riesgo	6 B Zona de Riesgo Importante Reducir el Riesgo Evitar el Riesgo Compartir o transferir	9 C Zona de Riesgo Inaceptable Evitar el riesgo Reducir el Riesgo Compartir o transferir		
		Posible	2	2 D Zona de Riesgo Tolerable Asumir el Riesgo Reducir el Riesgo	4 E Zona de Riesgo Moderado Reducir el riesgo Evitar el Riesgo Compartir o transferir	6 F Zona de Riesgo Importante Reducir el Riesgo Evitar el Riesgo Compartir o transferir
				Remoto	1	1 G Zona de Riesgo Aceptable Asumir el Riesgo
Impacto	Poco Significativo	Significativo	Muy Significativo			
	Valor	1	2	3		

Una vez se tienen las diferentes matrices de priorización, se deben extraer todos los riesgos que tengan una valoración de máxima, las cuáles por su importancia del riesgo o impacto y probabilidad o frecuencia de ocurrencia serán en un primer momento el conjunto de riesgos sobre el que se deben emprender acciones inmediatamente.

Cuando se ubican los riesgos en la matriz se define:

- ✓ Cuadrante C, B y F: Que por tanto requieren de la implementación de acciones a fin de aminorarlos tanto como se pueda o eliminarlos.
- ✓ Cuadrante G: Estos no requieren que se emprendan acciones inmediatas pero sí que se dejen establecidos a fin de hacerles seguimiento a través del tiempo.
- ✓ Cuadrante A, D, E, I y H: Estos riesgo deben ser tenidos en cuenta al iniciar cada año en los procesos anteriormente mencionados a fin de establecer el estado en el que se encuentre. Es posible que se mantengan en igual condiciones o que haya aumentado

su impacto y probabilidad de ocurrencia de donde se derivaría la implementación de acciones sobre ellos.

6.8.5 MONITOREO Y CONSULTA

Una vez diseñado y validado el plan para administrar los riesgos, es necesario monitorearlo permanentemente teniendo en cuenta que estos nunca dejan de representar una amenaza para la entidad, el monitoreo es esencial para asegurar que dichos planes permanecen vigentes y que las acciones están siendo efectivas.

Evaluando la eficiencia en la implementación y desarrollo de las acciones de control, es esencial adelantar revisiones sobre la marcha del plan de manejo de riesgos para evidenciar todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones preventivas.

El monitoreo estará a cargo de la Unidad de Riesgos en conjunto con cada responsable de los diferentes Departamentos, es decir, los dueños de los procesos y “riesgos” y su finalidad principal será la de aplicar los correctivos y ajustes necesarios para asegurar un efectivo manejo del riesgo.

La Unidad de Riesgos, se encargará de comunicar luego de monitorear o supervisar los hallazgos encontrados en las Unidades y realizará las sugerencias para el mejoramiento y tratamiento de los riesgos detectados así como de los riesgos residuales que se generen.

Durante las actividades de monitoreo se realizarán reuniones periódicas en donde se autoevaluará el comportamiento del riesgo y sí se han presentado nuevos riesgos dentro de la entidad que deban ser combatidos. Ésta autoevaluación no debe estar pensada como el fin del proceso, sino que muy por el contrario, nos entregará información importante para reformular el tratamiento de riesgos detectados, agregar nuevas acciones para combatirlos y a su vez generar dentro de las diferentes Unidades un ambiente de compromiso, y posibilitar a través de la retroalimentación el mejoramiento en el logro de los objetivos institucionales.

6.8.6 DOCUMENTACIÓN SOPORTE DE LA GESTIÓN DE RIESGOS

La Gestión de Riesgos se deberá soportar en una serie de documentos que evidenciarán su constitución y funcionamiento. Entre los principales documentos que deben integrarla se encuentra:

- Manual de Gestión de Riesgos.
- Definición de funciones y responsabilidades dentro de la Gestión de Riesgos.
- Políticas y Procedimientos de identificación, evaluación y tratamiento del riesgo.
- Plan anual de capacitación de cultura de riesgo.
- Políticas, procedimientos de supervisión y auditoría de la efectividad de los tratamientos establecidos para gestionar el riesgo.
- Mapa de Riesgo de la entidad.
- Mapa de Riesgo por Departamento.
- Informes y Actas de las reuniones periódicas
- Base de Datos de eventos de riesgo.
- Papeles de trabajo de Encuestas, entrevistas, Workflows, etc.

6.8.7 GLOSARIO Y DEFINICION DE TERMINOS

Administración de riesgos: Conjunto de objetivos, políticas, procedimientos y acciones que se implementan para identificar, medir, monitorear, limitar, controlar, informar y divulgar los distintos tipos de riesgo a que se encuentran expuestas las entidades financieras.

Análisis de riesgo: Evaluación sistematizada de la información que permite determinar la frecuencia de eventos de riesgo especificados y la magnitud del impacto.

Áreas funcionales: son las distintas unidades de la entidad que toman riesgos tales como la unidad de créditos, de tesorería y otras.

Área de registro: es la unidad encargada del procesamiento contable y de la verificación de la información utilizada por las áreas de negocios.

COSO: El seguimiento de la metodología COSO (Committee of Sponsoring Organization of the Traeway Comisión) inciden en el proceso de identificación de actividades críticas y riesgos potenciales inherentes a los procesos administrativos y de negocios.

Directorio: Toda referencia al directorio, entiéndase realizada a cualquier órgano equivalente.

Eventos externos: Aquellos sobre los que la entidad no tiene influencia pero que pueden afectar sus actividades

Frecuencia de Ocurrencia: Probabilidad de ocurrencia de fallo, ausencia, uso inadecuado

Impacto: Efecto del evento de riesgo sobre la actividad de la entidad

Información: Cualquier forma o conjunto de datos que se encuentran en formato electrónico, óptico, magnético o en otros medios, susceptible de ser procesada, distribuida y almacenada

Límites de Exposición: Exposición aceptada por la entidad financiera como nivel máximo de riesgo que determina puede soportar sin verse afectada.

Mapeo: identificación de riesgos en base a una evaluación gráfica que se sustenta en la lógica del análisis de procesos y en estimaciones cuantitativas y cualitativas.

Modelos Internos: Mecanismos de medición de riesgo diseñados por la misma entidad de financiera o por terceros que permite en el caso de riesgos identificar la probabilidad de incumplimiento, la pérdida dado el incumplimiento, la exposición a pérdidas y el logro de objetivos

Servidores Públicos: funcionarios, empleados y otros que desempeñen cargos o realicen labores dentro de la entidad.

Proceso: Conjunto de actividades, tareas y procedimientos organizados y repetibles, que consumen insumos o recursos y entregan un producto.

Proceso Clave: Proceso considerado indispensable para la continuidad de las operaciones y servicios de la empresa, y cuya falta o ejecución deficiente puede tener un impacto significativo en la empresa

Riesgo Institucional: Conjunto de riesgos que inciden sobre la actividad principal o sustantiva de la entidad financiera incluye a todos los riesgos aplicables riesgo de crédito, riesgo de mercado, riesgo de liquidez, riesgo operacional, riesgo legal, entre otros.

Riesgo Legal: Pérdida potencial por el incumplimiento de las disposiciones legales y administrativas aplicables, la emisión de resoluciones administrativas y judiciales desfavorables y la aplicación de sanciones, en relación con las operaciones que este tipo de entidades llevan a cabo.

Riesgo de Liquidez: Pérdida potencial por la disminución de activos por causas inusuales para hacer frente a sus obligaciones, o bien, por el hecho de que una posición no pueda ser oportunamente cubierta mediante el establecimiento de una posición contraria equivalente.

Riesgo Operativo: Pérdida potencial por fallas o deficiencias en los sistemas de información, en los controles internos o por errores en el procesamiento de las operaciones. El riesgo operacional tiene efectos en el logro de los objetivos institucionales como resultado de errores producto de fallas humanas, deficiencias en los controles internos o fallos de los sistemas implantados; que incluye riesgo de robo, fraude o estafa por parte de clientes, representantes, empleados o directivos.

Transferencia de riesgos: Cambiar la responsabilidad, prelación o carga por las pérdidas a un tercero quien asume la totalidad o parte de los riesgos.

CAPITULO IV CONCLUSIONES Y RECOMENDACIONES

1. CONCLUSIONES

Luego de revisar los documentos técnicos y la normativa legal relativa a la gestión del riesgo en el Sector Público Boliviano, es que se propone este documento como propuesta para su implementación en las entidades del Sector Público Financiero no Bancarias, como son los fondos y programas que administran recursos de financiamiento externo e interno, sin embargo puede ser también utilizado por otras entidades públicas para mejorar su gestión pública.

No existe normativa técnica específica sobre la gestión de riesgos, escasamente las Guías de Control Interno emitidos por la Contraloría General del Estado establecen evaluaciones del riesgo con un enfoque de control interno y solo para fines de auditoría que no son aplicados, por otro lado no existe disposición legal como la Ley 1178 SAFCO que tiene un enfoque de sistemas pero no considera a la gestión de riesgos como parte de los sistemas de administración, sino esta implícito en el sistema de control gubernamental, debido a que la gestión de riesgos es “preventiva”, se considera que es una evolución natural del enfoque de control interno que es “reactivo”, porque permite anticiparse a los errores o irregularidades por fallos en los procesos, personas y uso de la tecnología.

La tendencia de la Gestión Pública y Privada a nivel mundial se esta orientando a administrar los riesgos como parte de los procesos y estrategias institucionales, porque como entidades o empresas están expuestos y dificultan el logro de sus objetivos, y para ello es necesario tener una directriz o marco principal para la gestión del riesgo aplicable en las entidades del sector público financiero no bancario estableciendo Principios, una Estructura o Marco para su implementación y los Procesos de Gestión de riesgos, para un adecuado manejo de los riesgos que favorecerá al desarrollo y crecimiento de las entidades, y para asegurar dicho manejo debe considerarse el entorno en el que se desenvuelve la entidad.

La implementación total de la Gestión de Riesgos Operativos en estas entidades financieras permitirá conocer la realidad de como está la entidad en cuanto a los controles existentes, sus

CAPITULO IV Conclusiones y Recomendaciones

falencias, debilidades, si el diseño es adecuado o no, la verificación de si existe incumplimiento a normativa legal, etc.

Por otro lado, la prioridad, la experiencia y la criticidad de los eventos de riesgo en los procesos, personas y tecnología de información y su adecuado manejo en la gestión de las entidades, logrará convertirlas en entidades confiables y transparentes donde los servidores públicos, clientes, entidades tutoras y de control puedan confiar en que estas entidades del sector público financiero no bancario y los servicios y/o productos que brindan a la sociedad serán los adecuados y sostenibles para que en el marco del Plan de Desarrollo Regional y la nueva Constitución Política del Estado se logre el “VIVIR BIEN”.

Debido a que estas entidades administran recursos financieros importantes para el financiamiento de proyectos de inversión pública con la Administración o Gestión de Riesgos Operativos se debe buscar la excelencia máxima y lograr además la confianza de sus clientes, control social, organismos financiadores y resto del Gobierno, para todos los servicios que brinda, y demostrar si ocurriesen eventos de riesgo de cualquier impacto estarían preparados a sobrellevarlos de una forma eficiente logrando minimizar pérdidas y cualquier impacto en el cumplimiento de objetivos de la entidad financieramente y operativamente.

2. RECOMENDACIONES

Durante el desarrollo del proyecto, pude observar que estas entidades no toman conciencia de los riesgos a los que hoy en día están expuestos según su actividad y pero aún que las entidades del sector Público Financiero Bancario Financiero desconocen de la Gestión de Riesgos Operacionales, estas entidades en general deberían adoptar las recomendaciones de mejores prácticas de gestión de riesgos, especialmente a los que implican una pérdida financiera y que afecten al logro de sus objetivos y uno de los más importantes es financiera proyectos de inversión pública.

Estas entidades se dedican a administrar los recursos que les son otorgados con el enfoque de la Ley 1178 SAFCO, es decir, en base al modelo de control gubernamental previo, posterior, interno y externo, que ocasiona descuido en la operativa de sus procesos, y de acuerdo a lo expuesto es que se pretende que adapten los concepto técnicos de la gestión de riesgos en base

CAPITULO IV Conclusiones y Recomendaciones

al documento propuesto como **Manual de Riesgo Operativo**, donde se establecen los principios, marco y proceso de la gestión de riesgos, para que se inicie el proceso de implementación de un proceso de gestión del riesgo operativo en estas entidades.

Durante su implementación que se descubrirá que existen muchas cosas que no se hacen la forma más correcta, se incumplen o en fin hasta podrían hacer uso indebido de los recursos que le otorga a estas entidades, etc. por ello es necesario una reflexión y cambio del paradigma de control interno al de gestión de riesgos para ser eficientes, y dar la importancia de gestionar la operativa para el logro de objetivos institucionales, como en el caso de estas entidades es el de **Financiar**.

Con el fin de que se constituya un proceso continuo la gestión de riesgo operativo dentro de estas entidades, en base a lo establecido por el órgano rector del sistema de control gubernamental y de acuerdo a las necesidades institucionales, se recomienda:

- 1) Establecer una cultura de gestión de riesgo en las entidades, en remplazo a la lógica o cultura de control interno, para ello se requiera capacitación a las diferentes áreas.
- 2) Que la gestión de riesgos sea parte de la planificación estratégica y sea un proceso continuo y permanente, para ello el marco o estructura de la gestión de riesgo tiene que estar formalizada y aprobada por la Dirección Ejecutiva o instancia competente.
- 3) El uso de un sistema informático y creación de bases de datos de eventos de riesgo para una adecuada gestión de los riesgos con el fin de tener información oportuna, confiable y útil.

BIBLIOGRAFIA

Prácticas Sanas para la Administración y Supervisión del Riesgo Operativo

Comité de Basilea de Supervisión Bancaria
Banco de Pagos Internacionales - 2003

El Nuevo Acuerdo de Capital de Basilea

Comité de Basilea de Supervisión Bancaria
Banco de Pagos Internacionales - 2001

La Gestión del Riesgo Operacional – De la Teoría a su Aplicación.

Ana Fernandez Laviada
Ed. Ediciones 2010 - 2007

Gestión del Riesgo Operacional

Mariano Bas Uribe, José Manuel Delgado Calatrava
Ed. Dykinson – 2002

Administración de Riesgos E.R.M. y la Auditoría Interna

Rodrigo Estupiñán Gaitán
Ed. ECOE EDICIONES – 2006

Principios, Normas Generales y Básicas de Control Interno Gubernamental – CI/08

Contraloría General de la República de Bolivia
Versión 2 - Febrero 2007

Guía para la aplicación de los principios, normas generales y Básicas de Control Interno Gubernamental – CI/10

Contraloría General de la República de Bolivia
Versión 1 - Diciembre 2002

Guía Para la Implantación del Control Interno G/CE-021

Contraloría General de la República de Bolivia
Versió1 - Diciembre 2008

Guías para la Gestión de Riesgos

Superintendencia de Bancos y Entidades Financieras de Bolivia
PROFIN
Julio 2008

Buenas Prácticas para la administración del riesgo operacional en entidades financieras

Miguel Delfiner, Ana Mangialavori y Critian Pailhé

Enero 2007

Guía para las Normas del Control Interno del Sector Público – Información adicional sobre la Administración de Riesgos de la Entidad

Sub-Comité de Normas de Control Interno de la INTOSAI PSC

INTOSAI GOV 9130

2007

Auditoría Basada en Riesgos – Perspectiva estratégica de sistemas

Timothy Bell, Mark E. Peecher, Ira Solomon Frank O. Marrs, Howard Thomas

Ed. ECOE EDICIONES – 2007

Risk Management AS/NZS 4360:2004

Standards Australia/Standards New Zealand

2004

ISO 31000 Risk Management – Principles and guidelines

International Standard ISO/FDIS 31000:2009

ISO 2009 – All rights reserved