



**AGROBOLSA S.A.
MANUAL DEL SISTEMA DE ADMINISTRACION DEL RIESGO OPERATIVO
(SARO) DE LA COMPAÑIA**

VERSIÓN 2.0

Abril de 2010

Información del documento:

Documento:	Manual del Sistema de administración del riesgo operativo (SARO) de la Compañía.
Versión:	V 2.0
Fecha:	Abril de 2010
Autor(s):	Agrobolsa S.A.

Versión	Fecha	ACTA	Revisión/ Razón del cambio y alcance del mismo	Autor(s)
Primera	Junio 04 de 2007	No. 66	Aprobación Manual SARO Designación Comité Unidad de Riesgo Operativo	Asesores Externos: Value Markers
	Agosto 14 de 2007	No. 69	Modificación Manual Numeral 4.5. y 4.11.1.	Asesores Externos: Value Markers
Segunda	Abril 07 de 2010	No. 104	Actualización aspectos generales del Manual	Comité de Expertos: Auditor Interno, Contralor Normativo, Oficial de Cumplimiento

TABLA DE CONTENIDO	PAGINA
1. DEFINICION DE CONCEPTOS.....	7
2. OBJETIVOS Y POLÍTICAS PARA EL SISTEMA DE ADMINISTRACIÓN DEL RIESGO OPERATIVO.	9
3. ESTRUCTURA DEL SISTEMA DE ADMINISTRACIÓN DEL RIESGO OPERATIVO (SARO).....	10
3.1. Funciones y responsabilidades de la Junta Directiva	10
3.2. Funciones y responsabilidades del Gerente General de la Compañía	10
3.3. Funciones y responsabilidades del Comité de Riesgos	11
3.4. Organos de Control	<u>113</u>
4. METODOLOGÍAS PARA LA ADMINISTRACIÓN DEL RIESGO OPERATIVO	14
4.1. Identificación de los factores de Riesgo Operativo.....	14
Clasificación de los eventos de pérdida por proceso.....	15
4.2.1. Identificación de procesos	15
4.2.2. Identificación de eventos de pérdida y controles	16
4.3. Criterios de identificación de eventos de pérdida:.....	17
4.3.1. Criterios de identificación de controles y planes de contingencia	18
4.4. Medición del Riesgo Operativo.....	21
4.4.1. Primera etapa: Uso de escalas con rangos de valoración.....	21
<u>4.4.1.1. Riesgo Inherente, cluster de controles y planes de contingencia</u>	<u>21</u>
4.4.1.2. Riesgo Residual.....	<u>25</u>
4.4.2. Segunda etapa: Redes Bayesianas.....	25
4.5. Perfil de Riesgo.....	27
4.6. Matrices de Riesgo Operativo (ORM).....	28

4.7. Riesgo Legal	29
4.8. Riesgo Reputacional	29
4.8.1. Metodologías para monitorear y controlar el riesgo reputacional	30
4.9. Reporte de eventos de pérdida	32
4.10. Niveles de aceptación del riesgo operativo	32
4.11. Registro de eventos de riesgo operativo	33
4.11.1. Metodología y procedimiento para implementar y mantener el Registro de eventos de Riesgo Operativo.....	35
4.12. Procedimientos para el monitoreo y control del riesgo operativo	37
4.12.1. Alertas tempranas	37
4.12.2 Indicadores de Gestión	38
4.12.3. Controles.....	39
4.12.4. Nuevos procesos o modificación de procesos existentes.....	40
4.12.5. Procesos para administrar la continuidad del negocio.....	40
4.11.6. Gobierno Corporativo	41
4.12.7. Cultura de riesgos.....	41
4.12.8. Coordinación de comunicaciones.....	41
4.12.9. Canales de modificaciones de condiciones claros entre la Compañía y sus empleados y/o Clientes.....	42
4.12.10. Planes de Contingencia	42
4.12.11. Reportes internos y externos	43
5. PLATAFORMA TECNOLÓGICA	44
6. REVELACION CONTABLE.....	45
7. CAPACITACION Y DIVULGACION	45
8. Anexos.....	46

INTRODUCCION

El presente manual define los componentes de la estructura para la administración del Riesgo Operativo de Agrobolsa S.A., de acuerdo con lo dispuesto en la Circular Externa 049/06 de la Superintendencia Financiera sobre el Sistema de Administración del Riesgo Operativo (SARO).

Elementos que lo componen:

Los elementos para la administración del riesgo Operativo son: las políticas, objetivos, estructura organizacional, estrategias, procesos y procedimientos, que serán aplicados dentro del proceso de implementación y seguimiento del SARO dentro de la compañía, con base en lo establecido por la Superintendencia Financiera.

Area de aplicación:

Este Manual aplica para todos los empleados de la Compañía, establece y unifica las responsabilidades específicas del Comité de Riesgos, en lo concerniente a las funciones establecidas para la administración del Riesgo Operativo, la administración del riesgo SARLAFT, los riesgos comerciales y de la ejecución de los negocios.

El cumplimiento de lo descrito en el presente manual es obligatorio para todos los funcionarios que tengan relación con las actividades incluidas en él. Los desacatos darán lugar a llamados de atención por parte de la Gerencia de la compañía, sin perjuicio de las sanciones legales a las cuales haya lugar.

Aprobación y actualización del Manual:

El presente documento debe ser presentado para su aprobación a la Junta Directiva y a la Gerencia. El Comité de Riesgos debe velar porque el mismo se actualice por lo menos anualmente.

Objetivos del Manual:

El objetivo general del presente Manual es determinar las características del riesgo operativo y la forma de identificarlo, medirlo, monitorearlo y controlarlo dentro de la Compañía, con el fin de mitigar el impacto negativo de este riesgo sobre Agrobolsa S.A. y sobre su actividad y resultados financieros.

Los objetivos específicos del Manual son los siguientes:

- Dar cumplimiento a lo establecido en la Circular Externa 049/06 expedida por la Superintendencia Financiera, en lo que respecta al desarrollo e implementación del Sistema de Administración del Riesgo Operativo (SARO).
- Determinar las políticas de administración del riesgo operativo.
- Determinar las responsabilidades al interior de la Compañía y de sus funcionarios, en relación con el riesgo operativo.
- Identificar las principales fuentes del riesgo operativo para la Compañía.
- Establecer un procedimiento para su medición, en términos de impacto y probabilidad de ocurrencia.
- Establecer un procedimiento para su monitoreo y control.



1. DEFINICION DE CONCEPTOS

Riesgo Operativo: En términos de la Circular Externa 049/06 de la Superintendencia Financiera, se entiende por riesgo operativo, la posibilidad de incurrir en pérdidas por los siguientes factores: deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. Esta definición incluye el riesgo legal y reputacional, asociados a tales factores.

Factores de riesgo operativo: Son las fuentes generadoras de eventos en las que se originan las pérdidas por riesgo operativo.

De acuerdo con la clasificación general establecida en la Circular Externa 049 de 2006 de la Superintendencia Financiera, los factores de riesgo operativo se clasifican de la siguiente forma:

Factor Interno - Recurso Humano: Es el conjunto de personas vinculadas directa o indirectamente con la ejecución de los procesos de la Compañía.

Se entiende por vinculación directa, aquella basada en un contrato de trabajo en los términos de la legislación vigente.

La vinculación indirecta hace referencia a aquellas personas que tienen con la Compañía una relación jurídica de prestación de servicios diferente a aquella que se origina en un contrato de trabajo, como el caso del outsourcing.

Factor Interno - Procesos: Es el conjunto interrelacionado de actividades para la transformación de elementos de entrada en productos o servicios, para satisfacer una necesidad.

Factor Interno - Tecnología: Es el conjunto de herramientas empleadas para soportar los procesos de la Compañía. Incluye: hardware, software y telecomunicaciones.

Factor Interno - Infraestructura: Es el conjunto de elementos de apoyo para el funcionamiento de una organización. Entre otros se incluyen: edificios, espacios de trabajo, almacenamiento y transporte.

Factores externos: Son eventos asociados a la fuerza de la naturaleza u ocasionados por terceros, que escapan en cuanto a su causa y origen al control de la Compañía.

Eventos de pérdida: De acuerdo con la clasificación general establecida en la Circular Externa 049 de 2006 de la Superintendencia Financiera, son aquellos eventos que pueden originar pérdidas para la Compañía, como resultado de la presencia de uno o más de los anteriores factores de riesgo.

La clasificación de los eventos de pérdida es la siguiente:

Fraude interno: Son aquellas pérdidas derivadas de cualquier acto que de forma intencionada busca defraudar o apropiarse indebidamente de activos de la Compañía o incumplir normas, leyes o políticas empresariales en las que está implicado, al menos, un empleado o administrador de la Compañía, en beneficio propio o de un tercero.

Fraude externo: Son pérdidas derivadas de cualquier acto, realizado por una persona externa a la Compañía, que buscan defraudar, apropiarse indebidamente de activos de la misma o incumplir normas o leyes.

Relaciones laborales: Pérdidas derivadas de actos que son incompatibles con la legislación laboral, con los acuerdos internos de trabajo y, en general, la legislación vigente sobre la materia.

Clientes: Pérdidas derivadas del incumplimiento negligente o involuntario de las obligaciones frente a los clientes, que impiden satisfacer una obligación profesional frente a éstos.

Daños a activos físicos: Pérdidas derivadas de daños o perjuicios a activos físicos de la Compañía.

Fallas tecnológicas: Pérdidas derivadas de fallas tecnológicas.

Ejecución y administración de procesos: Pérdidas derivadas de errores en la ejecución y administración de procesos.

Adicionalmente, los anteriores eventos de pérdida pueden originarse como consecuencia de otros tipos de riesgo, como el legal y el reputacional.

Eventos de pérdida como consecuencia del Riesgo Legal: Por riesgo legal se entiende la posibilidad de pérdida en que incurre una entidad al ser sancionada, u obligada a indemnizar daños como resultado del incumplimiento de normas o regulaciones y obligaciones contractuales.

El riesgo legal surge también como consecuencia de fallas en los contratos y transacciones, derivadas de actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos o transacciones.

Eventos de pérdida como consecuencia del Riesgo Reputacional: Por riesgo reputacional se entiende la posibilidad de pérdida en que incurre la Compañía por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto de la institución y sus prácticas de negocio, que cause pérdida de clientes, disminución de ingresos o procesos judiciales.

2. OBJETIVOS Y POLÍTICAS PARA EL SISTEMA DE ADMINISTRACIÓN DEL RIESGO OPERATIVO

Los objetivos y políticas de la compañía para el Sistema de Administración de Riesgo Operativo son las siguientes:

- a. Crear un programa de capacitación, lo suficientemente amplio y permanente del Riesgo Operativo de la Compañía, de manera que todos los funcionarios adquieran el conocimiento adecuado y formen parte activa y responsable de su administración, teniendo en cuenta todos los procesos en los cuales participan.
- b. Involucrar activamente a todos los funcionarios de la Compañía, en la identificación y medición periódica de los eventos de pérdida, en forma técnica y uniforme, y de los controles que existen en los procesos a su cargo. Los resultados de estas actividades deben estar adecuadamente documentados.
- c. Identificar claramente las causas que originan los eventos de pérdida de la Compañía, con el fin de poder crear planes de acciones adecuados para su seguimiento y mitigación.
- d. Instaurar un proceso de administración de riesgo operativo que permita que su integración con los procesos propios de la Compañía sea fácil, de manera que los funcionarios puedan llevarlo a cabo de manera cotidiana, sin afectar su labor.
- e. Identificar amenazas y debilidades de los controles, en términos de su diseño y eficiencia, con el fin de proceder a mejorar su calidad, especialmente para aquellos riesgos cuyo impacto sobre la Compañía de llegar a ocurrir, es más grande.
- f. Contar con herramientas para mitigar o proteger a la Compañía de pérdidas considerables, por ejemplo alertas tempranas, sistemas de control congruentes con el nivel de riesgo de cada proceso, planes de contingencia e indicadores de gestión.

3. ESTRUCTURA DEL SISTEMA DE ADMINISTRACIÓN DEL RIESGO OPERATIVO (SARO)

3.1. Funciones y responsabilidades de la Junta Directiva

- a. Pronunciarse respecto de cada uno de los puntos que contengan los informes periódicos que presente el Gerente General.
- b. Pronunciarse sobre la evaluación periódica del SARO que realicen la Revisoría Fiscal y el Contralor Normativo.
- c. Proveer los recursos necesarios para implementar y mantener en funcionamiento, de forma efectiva y eficiente, el SARO.

3.2. Funciones y responsabilidades del Gerente General de la Compañía

- a. Diseñar y someter a aprobación de la Junta Directiva, el Manual de Riesgo Operativo y sus actualizaciones.
- b. Velar por el cumplimiento efectivo de las políticas establecidas por la Junta Directiva.
- c. Adelantar un seguimiento permanente de las etapas y elementos constitutivos del SARO que se llevan a cabo en la Compañía.
- d. Designar el área o cargo que actuará como responsable de la implementación y seguimiento del SARO: La Dirección de Riesgo (Comité de Riesgos).
- e. Desarrollar y velar porque se implementen las estrategias con el fin de establecer el cambio cultural que la administración de este riesgo implica para la Compañía.
- f. Adoptar las medidas relativas al perfil de riesgo, teniendo en cuenta el nivel de tolerancia al riesgo, fijado por la Junta Directiva.
- g. Velar por la correcta aplicación de los controles del riesgo inherente, identificado y medido.
- h. Recibir y evaluar los informes presentados por el Comité de Riesgos, de acuerdo con los términos establecidos en el presente Manual.

- i. Velar porque las etapas y elementos del SARO cumplan, como mínimo, con las disposiciones señaladas en la Circular Externa 049/06 de la Superintendencia Financiera.
- j. Velar porque se implementen los procedimientos para la adecuada administración del riesgo operativo a que se vea expuesta la Compañía en desarrollo de su actividad.
- k. Aprobar los planes de contingencia y de continuidad del negocio y disponer de los recursos necesarios para su oportuna ejecución.
- l. Presentar un informe periódico, como mínimo semestral, a la Junta Directiva sobre la evolución y aspectos relevantes del SARO, incluyendo, entre otros, las acciones preventivas y correctivas implementadas o por implementar y el área responsable.
- m. Establecer un procedimiento para alimentar el registro de eventos de riesgo operativo, de acuerdo con lo previsto en el presente Manual.
- n. Velar porque el registro de eventos de riesgo operativo cumpla con los criterios de integridad, confiabilidad, disponibilidad, cumplimiento, efectividad, eficiencia y confidencialidad de la información allí contenida.

3.3. Funciones y responsabilidades del Comité de Riesgos

El Comité de Riesgos estará conformada por la Gerente General Agrobolsa, el Oficial de Cumplimiento, el Subgerente Comercial, el Jefe de Contabilidad, el Contralor Normativo y el presidente de la Junta Directiva quienes ejecutarán todas las funciones dispuestas por la Superintendencia Financiera para la administración del Riesgo Operativo, las cuales se describen a continuación:

- a. Establecer las políticas relativas al SARO.
- b. Aprobar el Manual de Riesgo Operativo y sus actualizaciones.
- c. Hacer seguimiento y pronunciarse sobre el perfil de riesgo operativo de la Compañía.
- d. Establecer las medidas relativas al perfil de riesgo, teniendo en cuenta el nivel de tolerancia al riesgo de la Compañía, fijado por la Junta Directiva.
- e. Capacitarse dentro del Comité periódicamente en temas relacionados con la Administración del Riesgo Operativo, con el fin de poder desarrollar cabalmente sus funciones.

- f. Solicitar a la Junta Directiva los recursos necesarios para poder realizar adecuadamente su labor.
- g. Mantener su independencia de los órganos de control de la Compañía, y de las áreas de operaciones y de tecnología (Dirección Comercial y de Negocios).
- h. Informar cualquier relación entre sus miembros y las diferentes áreas de la Compañía, que originen conflictos de interés en lo que respecta a la administración del riesgo operativo.
- i. Definir los instrumentos, metodologías y procedimientos tendientes a que la Compañía administre eficientemente sus riesgos operativos, en concordancia con los lineamientos, etapas y elementos mínimos previstos en la Circular Externa 049/06 expedida por la Superintendencia Financiera.
- j. Identificar las fuentes que pueden generar situaciones de riesgo operativo al interior de la Compañía y clasificarlas por categorías que reflejen su importancia dentro de la entidad.
- k. Establecer un sistema de alerta temprana para anticiparse a potenciales pérdidas derivadas de situaciones de riesgo operativo dentro de la Compañía.
- l. Establecer y desarrollar los modelos de medición y evaluación del riesgo operativo y velar por su correcta implementación y funcionamiento.
- m. Desarrollar e implementar el sistema de reportes, internos y externos, del riesgo operativo de la Compañía.
- n. Administrar el registro de eventos de riesgo operativo.
- o. Coordinar la recolección de la información para alimentar el registro de riesgo operativo.
- p. Evaluar el impacto de las medidas de control potenciales para cada uno de los eventos de riesgo identificados y medidos.
- q. Establecer y monitorear el perfil de riesgo individual y consolidado de la Compañía y sus procesos, e informarlo a la Junta Directiva, en los términos del presente Manual.
- r. Realizar el seguimiento permanente de los procedimientos y planes de acción relacionados con el SARO y proponer sus correspondientes actualizaciones y modificaciones.

- s. Desarrollar los programas de capacitación de la Compañía relacionados con el riesgo operativo y el SARO.
- t. Realizar seguimiento a los controles, planes de contingencia y medidas adoptados para mitigar el riesgo inherente, con el propósito de velar por su cumplimiento y evaluar su efectividad.
- u. Determinar el tipo de control a aplicar al riesgo inherente, identificado y medido.
- v. Reportar semestralmente al Representante Legal de la Compañía, la evolución del riesgo, su medición, los controles implementados y el monitoreo que se realice sobre el mismo, en los términos de la Circular Externa 049/06 expedida por la Superintendencia Financiera.
- w. Establecer las metodologías y procedimientos necesarios para el continuo monitoreo y mitigación del riesgo operativo, mediante elementos como: desarrollar indicadores de gestión, proponer nuevos controles o mejorar los controles existentes, y evaluar los planes de contingencia elaborados por cada área.

3.4. Órganos de Control

El órgano de control interno dispuesto para evaluar el SARO dentro de la compañía será el Contralor Normativo, quien sin perjuicio de sus otras funciones asignadas, determinará las fallas, inconsistencias e incumplimientos del sistema y deberá informar de estos a la Junta Directiva y a la Gerencia General.

La instancia de control anteriormente mencionada no será responsable de la Administración del Riesgo Operativo y sus funciones tienen alcance únicamente para ejercer la evaluación del sistema. Para tal fin todas las áreas dentro de la Compañía deben atender sus solicitudes y requerimientos para cumplir a cabalidad el objetivo de su función.

De considerarlo necesario la Compañía podrá contratar asesores y/o auditores externos especializados en gestión de riesgos, para fortalecer la labor de los órganos de control en la evolución y/o evaluación del SARO.

Funciones del Contralor Normativo en la evaluación del SARO:

Evaluar periódicamente la efectividad y cumplimiento de todas y cada una de las etapas y los elementos del SARO con el fin de determinar las deficiencias y sus posibles soluciones.

Informar los resultados de la anterior evaluación del Comité de Riesgos y al Gerente General.

Realizar una revisión periódica del registro de eventos de riesgo operativo e informar al Gerente General sobre el cumplimiento de las condiciones señaladas para el mismo en la Circular Externa 049/06 de la Superintendencia Financiera.

Funciones de la Revisoría Fiscal en la evaluación del SARO:

Elaborar un reporte al cierre de cada ejercicio contable en donde se informen conclusiones obtenidas en el proceso de evaluación del cumplimiento de las normas e instructivos sobre SARO.

Poner en conocimiento del Gerente General, los incumplimientos del SARO, sin perjuicio de la obligación de informar sobre ellos a la Junta Directiva.

4. METODOLOGÍAS PARA LA ADMINISTRACIÓN DEL RIESGO OPERATIVO

Las metodologías para la administración del riesgo operativo están compuestas por las actividades de identificación, medición, monitoreo y control de riesgos. A continuación se describen cada una de estas actividades:

4.1. Identificación de los factores de Riesgo Operativo

De acuerdo con la clasificación establecida por la Superintendencia Financiera, los siguientes son los factores de riesgo operativo que Agrobolsa S.A. utilizará en sus matrices de Riesgo Operativo:

Factor Interno - Recurso Humano
Factor Interno – Procesos
Factor Interno – Tecnología
Factor Interno – Infraestructura
Factores externos

Así mismo, de acuerdo con la clasificación establecida por la Superintendencia Financiera, los siguientes son los eventos de pérdida que Agrobolsa S.A. utilizará en sus matrices de Riesgo Operativo:

CLASIFICACION PRIMER NIVEL

Fraude interno
Fraude externo
Relaciones laborales
Clientes
Daños a activos físicos

Fallas tecnológicas
Ejecución y administración de procesos

Con el fin de poder llevar a cabo un mejor seguimiento y valuación de los eventos de pérdida, Agrobolsa S.A. creará un segundo nivel de clasificación de eventos de pérdida o subclasificación, más detallado.

Clasificación de los eventos de pérdida por proceso

El objetivo de las clasificaciones y subclasificaciones de los eventos de pérdida por proceso, es asegurarse de que no hay debilidades o inadecuaciones en el medio ambiente general de riesgo, que permitan a un riesgo en particular provocar una pérdida significativa para la Compañía. Los eventos de pérdida responden a la pregunta: ¿Qué podría salir mal?

La elaboración y mantenimiento actualizado de este segundo nivel o subcategorías de eventos de pérdida, es labor del Comité de Riesgos, con el apoyo de los funcionarios de las diferentes áreas de la Compañía.

Para ello, se debe realizar el siguiente procedimiento:

4.2.1. Identificación de procesos

Partiendo de los procesos identificados dentro de la Compañía, debe existir un dueño de proceso asignado a cada uno de ellos. En caso de no existir todavía un dueño de proceso, tal asignación será efectuada por el Comité de Riesgos.

De acuerdo con la Circular Externa 049/06 expedida por la Superintendencia Financiera, un proceso es el conjunto interrelacionado de actividades para la transformación de elementos de entrada en productos o servicios, para satisfacer una necesidad, tanto interna como externa.

El dueño del proceso es el responsable por administrar el proceso entero (Cabeza del proceso). Su función dentro de la administración de riesgos es la de revisar el nivel de evaluación del riesgo del respectivo proceso, para asegurarse de que esté completo y abarque todo el proceso, y de que el proceso esté vigente y los subprocesos y actividades que lo componen, estén actualizados.

Esta labor resulta particularmente importante, cuando se han presentado cambios significativos en el medio ambiente operativo de la Compañía.

El dueño del proceso debe identificar aquellos subprocesos que requieran de evaluación en términos de riesgo, y debe designar los miembros apropiados de su equipo, para ayudar a dimensionar los niveles de proceso y sus riesgos.

4.2.2. Identificación de eventos de pérdida y controles

En conjunto con los dueños de procesos, quienes actúan como facilitadores, los funcionarios involucrados en cada uno de los procesos y subprocesos (Los cuales deben encontrarse debidamente documentados), deben reunirse periódicamente, mediante talleres o sesiones de trabajo, de acuerdo con el cronograma que para tal efecto elabore el Comité de Riesgos y/o Asesores Externos, los participantes deben realizar las siguientes actividades

Estas reuniones, pueden llevarse a cabo con el apoyo del Comité de Riesgos y/o Asesores externos, los participantes deben realizar las siguientes actividades:

- a. Identificar los potenciales eventos de pérdida que se consideran relevantes dentro del proceso o subproceso, utilizando para ello su conocimiento y experiencia en dicho proceso o subproceso.
- b. Determinar eventos de pérdida predefinidos y relevantes, dentro del universo de eventos de pérdida. Esto significa, que dada la gran magnitud de eventos de pérdida posible, por ejemplo: terremotos, incendios, publicidad negativa sobre la empresa, huelgas, fallas en los aplicativos, hurtos, fraudes, etc., se deben seleccionar aquellos que los participantes consideren como los más relevantes para ese proceso o subproceso en particular.

Para ello, se parte de un universo de eventos de pérdida.

- c. Identificar adicionales eventos de pérdida relevantes del proceso o subproceso, que no estén cubiertos por el universo con que se cuenta previamente, y asignarlos a las subcategorías de factores de riesgo establecidas por el Comité de Riesgos.
- d. Identificar controles y la estrategia de asignación de controles que son usados al momento del análisis, para mitigar los riesgos del proceso o subproceso.
- e. Identificar la existencia y cobertura de los planes de contingencia para fallas en el proceso.
- f. Medir el impacto y frecuencia del riesgo inherente.

El riesgo inherente es definido como una medida realista y probable del evento de pérdida, anterior a cualquier control que pueda ser colocado en relación con dicho evento.

Para cada evento de pérdida relevante que se identifique, el impacto y frecuencia del riesgo inherente de dicho evento de pérdida debe ser evaluada

o medida. Para ello, se utiliza la metodología que se describe más adelante en el presente Manual.

- g. Evaluar el diseño y desempeño del Sistema de Control (La suma de todos los controles del proceso o subproceso) y los planes de contingencia.

Un control se define como una actividad que está en un lugar, para reducir el impacto o probabilidad de ocurrencia de un evento de riesgo.

Cada control y plan de contingencia debe evaluarse de acuerdo con la metodología que se describe más adelante en el presente Manual.

- h. Finalmente, los resultados de estos talleres o reuniones de trabajo deben documentarse y posteriormente ingresarse a las Matrices de Riesgo Operativo (ORM) administradas por el Comité de Riesgos, con la periodicidad y en las condiciones establecidas por dicha Gerencia.

Los resultados deben ser revisados previamente por el Comité de Riesgos, para asegurarse de que todos los eventos de pérdida relevantes sean incluidos, si bien no es imperativo que todos los escenarios de riesgo sean cubiertos a nivel de proceso/subproceso.

La revisión de determinados eventos de pérdida puede ser asignada a una función central.

4.3. Criterios de identificación de eventos de pérdida:

Los criterios que deben tener en cuenta los funcionarios involucrados en cada proceso, para realizar la identificación y clasificación de los eventos de pérdida de dicho proceso son:

- a. Cuantificar el número de veces en promedio mensual que realizan cada uno de los subprocesos o actividades de cada proceso. Este promedio mensual debe corresponder por lo menos a los últimos doce (12) meses. Los procesos se organizan luego en orden de frecuencia.
- b. Ordenar los subprocesos o actividades de acuerdo con la importancia que el dueño del proceso atribuya a los mismos como factores de éxito del proceso en conjunto; es decir, evaluando qué tanto afectan el resultado final del proceso, en caso de que estos subprocesos se realicen mal o no se realicen.
- c. Para cada proceso, el dueño del mismo debe establecer cuáles son los principales elementos utilizados por la Compañía para llevar a cabo dicho proceso. Estos elementos se clasifican en: recurso humano, recurso tecnológico, recurso físico y recurso de información.

El recurso humano hace referencia a los funcionarios que participan directamente en alguna parte del proceso, actuando concretamente en una o varias actividades del mismo.

El recurso tecnológico hace referencia a la utilización de software especializado durante el proceso, bien sea desarrollado por la Compañía o aquel perteneciente a un proveedor externo.

El recurso físico hace referencia a todos aquellos activos tangibles utilizados durante el proceso, incluyendo cualquier tipo de máquina no especializada o computadores con software no especializado.

El recurso de información hace referencia a los datos de entrada, tanto internos como externos, necesarios para realizar el proceso.

Por ejemplo, para el proceso denominado; Pago a Proveedores, se utiliza el recurso humano, representado en el funcionario encargado de elaborar los cheques y el o los funcionario(s) encargado(s) de firmarlos; el recurso físico, representado en los cheques físicos, la máquina de escribir o el computador para llenar cada cheque, los sellos y protectores utilizados para cada cheque; y el recurso de información, representado en el listado autorizado con los datos de los beneficiarios a quienes se debe girar cada cheque.

- d. Los elementos de cada proceso deben organizarse en orden de importancia de costo; es decir, ordenándolos de mayor a menor por el costo estimado, de cada uno de dichos elementos, para llevar a cabo un proceso en particular.
- e. Teniendo en cuenta la anterior información, se comienzan a identificar los eventos de pérdida, comenzando por aquellos subprocesos críticos según los anteriores criterios.

4.3.1. Criterios de identificación de controles y planes de contingencia

En primer lugar, deben identificarse el número y la clase de controles que existen en cada proceso, de acuerdo con la siguiente clasificación:

- a. Por su forma de funcionamiento

Manuales: Son aquellos controles efectuados directamente por las personas, sin la utilización de aparatos o sistemas.

Mecánicos: Son aquellos controles efectuados a través de aparatos, los cuales pueden requerir o no de su aplicación por parte de personas.

Automáticos: Son aquellos controles efectuados a través de sistemas, los cuales no requieren de la participación de las personas para su aplicación.

b. Por el momento de su aplicación

Previos: Son aquellos controles efectuados antes de iniciar el proceso.

Durante el proceso: Son aquellos controles efectuados periódicamente, a lo largo del proceso.

Posteriores: Son aquellos controles efectuados al finalizar un proceso, para verificar si el mismo cumplió o no con los parámetros establecidos.

c. Por su efecto sobre el riesgo

Preventivos: Son aquellos controles efectuados con el fin de reducir la probabilidad de que el riesgo se materialice.

Sobre resultados o Detectives: Son aquellos controles efectuados al finalizar un proceso, para verificar si el mismo cumplió o no con los parámetros establecidos. También se utilizan para aminorar el impacto negativo de un evento, una vez ocurrido.

De seguros o transferencia de riesgos: Son controles diseñados para mitigar el impacto de un evento de riesgo, una vez que el mismo ha ocurrido, pero orientado a reducir la pérdida o costo financiero.

d. Por el tipo de bien o proceso que controlan

Controles de sistemas: Incluye controles de usuarios, para establecer quién utiliza el sistema y si está autorizado para ello o no, así como controles para establecer la validez de las modificaciones y desarrollos efectuados a dichos sistemas o programas.

También incluye controles para el adecuado seguimiento a los errores, con el fin de establecer si los mismos son investigados y resueltos apropiadamente.

Controles de acceso físico: Tienen como objetivo proteger los activos de la Compañía, y restringir el acceso a determinadas áreas donde se encuentran activos o información que se considera de gran valor para la Compañía.

Controles de bases de datos, registros e información: Estos controles incluyen mecanismos para asegurar la correcta captura de datos en los aplicativos de la Compañía y mantener los datos libres de cualquier daño o modificación posterior.

Controles de personal: Establecidos para asegurar la calidad e integridad del personal que está encargado de ejecutar los métodos y procedimientos prescritos por la Compañía para el logro de los objetivos.

Controles de protección de activos: Este tipo de controles incluye el acceso físico a las diferentes áreas de la Compañía, así como el acceso restringido a los equipos, a la documentación y a los archivos de datos y programas, todo ello solo permitido al personal autorizado.

Controles de los equipos: Consiste en la programación del mantenimiento preventivo y periódico, el registro de fallas de equipos y los cambios en el sistema operativo y a programación del software utilizado por la Compañía.

Controles de procesos contables: Deben existir controles que aseguren el procesamiento exacto y oportuno de la información contable.

Controles de autorización: Consisten en la revisión de los intercambios, a nivel de cualquier proceso de la Compañía, para asegurar que estos hayan sido autorizados apropiadamente.

Controles de custodia de activos: Están diseñados para evitar que los activos se pierdan, dañen o sean robados, y proporcionar la seguridad de que las cantidades y los valores en existencia sean coincidentes con los registrados.

Incluye controles para prevenir el uso no autorizado sobre un activo durante su custodia.

Controles de estructura organizacional: Consisten en establecer una adecuada estructura en cuanto al establecimiento de divisiones y departamentos funcionales, así como la asignación de responsabilidades y políticas de delegación de autoridad.

Esto incluye la existencia de un departamento de control interno que dependa del máximo nivel de la Compañía.

Controles de organización: Buscan evitar que se inicien o autoricen intercambios de cualquier proceso, que no sean para suministros y servicios propios de la respectiva área.

Incluyen el Registro de los intercambios, custodia de activos que no sean del área respectiva, y corrección de errores que no provengan de los originados por el área respectiva.

Controles de separación de funciones: Están diseñados para verificar que cualquier proceso segregue las siguientes funciones:

- Comprometer a la Compañía en el intercambio del respectivo proceso.
- Aceptar o entregar el activo o el instrumento objeto del intercambio.
- Ingresar los datos del intercambio al sistema de procesamiento.

Estos controles también buscan evitar que se presente una combinación de funciones de una misma persona en relación con distintos tipos de intercambios.

Controles de conciencia de control: La Alta Gerencia es responsable del establecimiento de una conciencia favorable de control interno de la Compañía. Es importante que la Alta Gerencia no viole los controles establecidos porque el sistema es ineficaz.

La Alta Gerencia se podría motivar a violarlos por las siguientes causas:

- Cuando la Compañía está experimentando numerosos fracasos.
- Cuando le falte capacidad de capital de trabajo o financiación.
- Cuando la remuneración de la Alta Gerencia está ligada al resultado.
- Cuando la Alta Gerencia se encuentra bajo presión en cumplir sus objetivos.

Deben existir controles para impedir que la conciencia de control por parte de la Alta Gerencia, llegue a debilitarse o perderse.

En segundo lugar, deben identificarse los planes de contingencia existentes para el proceso, de la siguiente forma:

- Planes frente a la ausencia de personal
- Planes frente al sobrepaso de límites
- Planes frente a inconvenientes con recursos físicos
- Planes frente a inconvenientes con aplicativos y sistemas
- Planes frente a la falta de normatividad
- Planes frente a inconvenientes en los procesos

4.4. Medición del Riesgo Operativo

La medición del riesgo operativo se realiza en dos etapas.

4.4.1. Primera etapa: Uso de escalas con rangos de valoración

La primera etapa se realiza en los talleres, durante el proceso de identificación de los eventos de pérdida y los controles.

4.4.1.1. Riesgo inherente, cluster de controles y planes de contingencia:

En el caso de los eventos de pérdida, para cada uno de dichos eventos debe medirse el **impacto** y **frecuencia** del riesgo inherente.

Y en el caso de los controles, se debe evaluar el grado en que todos los controles están asignados a una estrategia de control adecuada.

Una estrategia de control representa una clasificación o tipo de control, dentro de los diferentes tipos de clasificaciones descritos anteriormente en el presente Manual.

La suma de controles y la clasificación a la que pertenecen; es decir, la estrategia de control, conforma lo que se denomina como el Sistema o Cluster de Control. Debido a la gran cantidad de controles que pueden existir para un evento de pérdida en particular, para efectos de la administración del riesgo se toman únicamente aquellos controles clave; es decir, aquellos que resultan más importantes para mitigar o reducir la posibilidad de ocurrencia del riesgo.

El Cluster de Control de cada uno de los eventos de pérdida, se evalúa en dos aspectos: Su **diseño** y su **efectividad**.

A continuación se describen los cuatro atributos: impacto, frecuencia, diseño y efectividad que se deben medir como parte del sistema de administración de riesgos de la Compañía.

Impacto: Atributo del evento de pérdida, que cuantifica la magnitud en pesos de la pérdida ocasionada por la ocurrencia de dicho evento.

Frecuencia: Atributo del evento de pérdida, que cuantifica el número de veces que un evento en particular se produce durante un periodo de tiempo determinado. Se puede expresar también en términos de su probabilidad de ocurrencia.

Diseño: Atributo del cluster de control o plan de contingencia, que califica la relevancia del mismo, en aspectos como la oportunidad del mismo, la no existencia de controles o planes de contingencia redundantes, la necesidad del mismo, la superioridad del mismo frente a otras alternativas de control o plan de contingencia, el nivel de cobertura del mismo, la regularidad en su aplicación, la experiencia y autoridad de los miembros de la Compañía que lo diseñaron, etc.

Dado que esta evaluación es cualitativa, debe existir un parámetro cuantitativo vinculado a dicha escala.

Efectividad: Atributo del cluster de control o plan de contingencia, que mide el efecto en pesos que logra dicho control o plan de contingencia, en términos de reducción de la impacto o frecuencia de ocurrencia del evento de pérdida.

Todos estos atributos son evaluados usando una escala compuesta por cinco rangos predefinidos. Esta escala es diseñada por el Comité de Riesgos. Esta escala es la misma para todos los eventos de riesgo.

Los rangos deben establecerse de manera que la evaluación no se concentre en un solo rango. Los rangos deben permitir una buena diversificación de los resultados. Como regla de aprobación, no menos del 10% de todas las calificaciones de eventos de pérdida deben estar en cada rango y no más del 35% en un solo rango.

Cada funcionario participante en el taller o reunión de trabajo, diligencia la escala y el resultado es promediado. Para poder realizar dicho promedio, cada rango debe contar con un punto medio, el cual es el resultado de sumar el punto inferior del rango y el punto superior del rango, y luego dividir el resultado entre dos.

Rating del riesgo inherente:

IMPACTO	IMPACTO DEL EVENTO EN MILLONES DE PESOS
MUY ALTO	Más 50
ALTO	Entre 31 y 50
MODERADO	Entre 16 y 30
BAJO	Entre 2 y 15
MUY BAJO	Entre 0 y 1

PROBABILIDAD DEL EVENTO	RANGO DE FRECUENCIA
MUY ALTO	81% - 100%
ALTO	61% - 80%
MODERADO	41% - 60%
BAJO	21% - 40%
MUY BAJO	1% - 20%

El rango inferior, tanto para la escala de impacto como para la escala de frecuencia, no necesariamente comienza en cero. Se puede establecer un nivel mínimo un poco mayor, lo que se interpreta como que aquellos eventos de pérdida cuya ocurrencia tenga una frecuencia o impacto menor a la de dicho límite, se consideran insignificantes y por lo tanto no se tendrán en cuenta en este análisis.

El rango superior es en teoría hasta el nivel de infinito. Sin embargo, con el fin de poder determinar un punto medio, se debe dar un valor que se considere suficiente y que pueda cambiarse en cualquier momento, si la ocurrencia de algún evento de pérdida lo supera.

En los demás aspectos, los rangos deben permanecer constantes a lo largo del tiempo, a menos que ocurran cambios importantes en el negocio. Finalmente, los rangos deben diseñarse en una forma exponencial, para que su agregación resulte en valores razonables.

Como resultado del anterior análisis, es posible que los participantes no identifiquen eventos de pérdida para una subcategoría de riesgo en particular. Esto es válido; sin embargo debe ser ratificado por el dueño del proceso y el Comité de Riesgos.

Una vez promediados los resultados, se obtiene una impacto promedio y una frecuencia promedio, para cada evento de pérdida en términos de riesgo inherente; es decir, antes de evaluar controles.

El último paso consiste en multiplicar la impacto promedio por la frecuencia promedio, lo que se denomina rating del riesgo inherente. Esto permite comparar unos eventos de pérdida con otros, al estar expresados en la misma base.

Rating del cluster del control:

La escala del cluster de control se construye de la misma forma que la escala del riesgo inherente, pero los valores deben estar entre 0 y 1. El objetivo es contar con porcentajes para aplicar al riesgo inherente y de esta forma hallar el riesgo residual, de la forma como se describe más adelante.

DISEÑO	CALIDAD DEL CONTROL
EXCELENTE	De un 81% a un 100%
BUENO	De un 61% a un 80%
REGULAR	De un 41% a un 60%
MALO	De un 21% a un 40%
PESIMO	De un 1% a un 20%

EFECTIVIDAD	RANGO DE COBERTURA DEL CONTROL
EXCELENTE	De un 81% a un 100%
BUENO	De un 61% a un 80%
REGULAR	De un 41% a un 60%
MALO	De un 21% a un 40%
PESIMO	De un 1% a un 20%

4.4.1.2. Riesgo residual:

Una aproximación numérica, basada en un análisis cualitativo, del riesgo residual, se obtiene al utilizar la siguiente ecuación:

$$\text{Riesgo Residual} = \text{Rating del Riesgo Inherente} * (1 - \text{Rating de Diseño Cluster de Control} * \text{Rating de Efectividad del Cluster de Control})$$

De esta forma, se obtiene como resultado final el valor en pesos del riesgo residual; es decir, el riesgo de un evento de pérdida teniendo en cuenta los controles existentes para mitigar o reducir dicho riesgo.

4.4.2. Segunda etapa: Redes Bayesianas

Esta segunda etapa aplica únicamente para el riesgo residual, ya que se basa en información estadística, la cual tiene la ventaja de permitir establecer conclusión a partir de casos realistas y evitar supuestos teóricamente válidos pero no en la realidad.

Como las estadísticas parten de situaciones reales históricas, las mismas contemplan controles en funcionamiento para los diferentes eventos de pérdida. No es posible por lo tanto contar con estadísticas de riesgo inherente puro o del efecto de los controles sobre dicho riesgo inherente.

Por lo tanto, las estadísticas apuntan a establecer dos principales escenarios del riesgo residual: El escenario típico y el escenario extremo.

Impacto típico del riesgo residual:

Corresponde al impacto esperado, calculado estadísticamente, del riesgo residual asociado a un evento de pérdida en particular.

Impacto extremo del riesgo residual:

Corresponde al impacto máximo, calculado estadísticamente, del riesgo residual asociado a un evento de pérdida en particular, con un nivel de confianza de mínimo el 95%.

Probabilidad de ocurrencia típica del riesgo residual:

Corresponde a la probabilidad de ocurrencia esperada, calculada estadísticamente, del riesgo residual asociado a un evento de pérdida en particular.

Probabilidad de ocurrencia extrema del riesgo residual:

Corresponde a la probabilidad de ocurrencia máxima, calculada estadísticamente, del riesgo residual asociado a un evento de pérdida en particular, con un nivel de confianza de mínimo el 95%.

Probabilidad de ocurrencia:

La probabilidad de ocurrencia se establece a partir del número de veces que se ha presentado un evento de pérdida en un proceso determinado en los tres años anteriores, información que debe estar contemplada en el Registro de eventos de Riesgo Operativo que la Circular Externa 049/06 expedida por la Superintendencia Financiera establece.

Luego de determinar el número de veces que se ha presentado el evento de pérdida, se divide este número de veces entre doce (12) meses y el resultado se divide nuevamente por el número de veces que se realiza el proceso en promedio al mes, esto último calculado de acuerdo el dato arrojado por el Registro de Eventos Operativos calculado por el Comité de Riesgos. El resultado es la probabilidad de ocurrencia del evento de pérdida.

De acuerdo con la probabilidad de ocurrencia establecida, cada uno de estos eventos se clasificará de la siguiente forma:

Probabilidad de ocurrencia

Alta:	Aquellos eventos de pérdida que en los últimos tres años, por lo menos, tienen una probabilidad de ocurrencia mayor a 0.50.
Media:	Aquellos eventos de pérdida que en los últimos tres años, por lo menos, tienen una probabilidad de ocurrencia entre 0.25 y 0.50.
Baja:	Aquellos eventos de pérdida que en los últimos tres años, por lo menos, tienen una probabilidad de ocurrencia menor a 0.25.

Impacto:

El impacto se establece a partir de los valores históricos de pérdida cuantificados al presentarse dicho evento dentro de un proceso determinado en los tres años anteriores, información que debe estar contemplada en el Registro de eventos de

Riesgo Operativo que la Circular Externa 049/06 expedida por la Superintendencia Financiera establece.

Luego de determinar el valor histórico de pérdida cuantificado al presentarse en cada ocasión dicho evento, se determina el valor promedio del mismo, sumando todos los valores de pérdida y dividiéndolos por el número de veces que se presentó dicho evento en el mismo lapso de tiempo. El resultado es la impacto esperada del evento de pérdida. De acuerdo con la impacto esperada, cada uno de estos eventos se clasificará de la siguiente forma:

Impacto esperado:

Impacto Crítico:	Aquellos eventos de pérdida que en caso de ocurrir, pueden generar en el mes una pérdida mayor al 5.00% del patrimonio total de la Compañía.
Impacto Alto:	Aquellos eventos de pérdida que en caso de ocurrir, pueden generar en el mes una pérdida de entre el 1.00% y el 5.00% del patrimonio de la Compañía.
Impacto Medio:	Aquellos eventos de pérdida que en caso de ocurrir, pueden generar en el mes una pérdida de entre el 0.50% y el 1.00% del patrimonio de la Compañía.
Impacto Bajo:	Aquellos eventos de pérdida que en caso de ocurrir, pueden generar en el mes una pérdida menor al 0.50% del patrimonio de la Compañía.

Las anteriores clasificaciones deben servir para determinar el perfil de riesgo de la Compañía; es decir, los criterios y estrategias de aceptación o traslado de riesgos.

El modelo utilizado para el cálculo estadístico será el de redes bayesianas. Las redes bayesianas son un modelo gráfico probabilístico, que representa un conjunto de variables y sus influencias causales o dependencias probabilísticas.

Dichas redes están conformadas por nodos y arcos, donde los nodos representan variables y los arcos presentan causas o dependencias probabilísticas entre variables.

La fortaleza de las dependencias está expresada por distribuciones de probabilidad condicional, vinculadas a cada nodo.

El Comité de Riesgos será la responsable de aplicar esta metodología, integrar sus resultados dentro de las Matrices de Riesgo que se elaboren y preparar informes periódicos, por lo menos una vez al año, a la Junta Directiva para informarle de los resultados obtenidos.

4.5. Perfil de Riesgo

El perfil de riesgo establecido para la Compañía, según la anterior metodología, se ubicará en alguna de los niveles de la siguiente escala:

Nivel de Riesgo Residual	Concepto	Perfil	Tratamiento
Muy Alto	Pone en peligro la continuidad del negocio de la Compañía.	Inaceptable. Debe informarse inmediatamente a la Alta Gerencia y a la Junta Directiva, quienes deben proporcionar los recursos inmediatos para su tratamiento. Requiere acción inmediata para regresarlo como máximo al Nivel Alto.	Transferir el riesgo vía seguros, evitar el riesgo eliminando su fuente (Línea de negocio) potencial originadora, reducir su impacto o probabilidad de ocurrencia vía planes de contingencia, controles y planes de continuidad de negocio.
Alto	Genera un impacto negativo, a nivel operativo y financiero, fuerte sobre la Compañía, pero sin poner en peligro la continuidad del negocio.	Gestionable. Debe informarse inmediatamente a la Alta Gerencia para que tome las medidas necesarias para su monitoreo y control permanente, determinando responsables a nivel Directivo para dicha labor.	Transferir el riesgo vía seguros, reducir su impacto o probabilidad de ocurrencia vía planes de contingencia y controles.
Medio	Genera un impacto moderado sobre la Compañía, que no afecta de manera importante su situación financiera u operativa.	Gestionable. Debe informarse oportunamente al Comité de Riesgos para que lleve a cabo un monitoreo periódico de dicho riesgo a través de los informes presentados por la Unidad de Riesgo Operativo y los responsables de cada área. Se deben evaluar controles y planes de contingencia existentes, buscando mejorarlos.	Transferir el riesgo vía seguros, reducir su impacto o probabilidad de ocurrencia vía planes de contingencia y controles.
Bajo	No genera mayor impacto negativo sobre la operación o finanzas de la Compañía.	Gestionable. Debe formar parte de los informes periódicos preparados por la Unidad de Riesgo Operativo al Comité de Riesgos. Requiere de su seguimiento mediante indicadores de alerta temprana, para evitar que su impacto o probabilidad aumenten. El enfoque de control debe ser de costo/beneficio.	Mantener bajo su impacto o probabilidad de ocurrencia vía planes de contingencia y controles.
Muy Bajo	Su impacto negativo es insignificante.	Enfoque de monitoreo de rutina, a cargo principalmente de los funcionarios a cargo del respectivo proceso.	Aceptarlo

4.6. Matrices de Riesgo Operativo (ORM)

Los factores de riesgo operativo, eventos de pérdida, cluster controles, planes de contingencia, riesgo inherente y riesgo residual, que se obtengan como resultado de los procesos de identificación y medición de riesgos descritos en el presente Manual, deberán registrarse y consolidarse en una Matriz de Riesgo Operativo (ORMA por sus siglas en inglés).

A partir de dichas Matrices de Riesgo Operativo y del Registro de eventos de riesgo operativo que se menciona más adelante, el Comité de Riesgos debe preparar un informe semestral a la Junta Directiva, donde manifieste su opinión acerca del adecuado funcionamiento y suficiencia de los controles y planes de contingencia establecidos para cada riesgo.

El Comité de Riesgos podrá proponer nuevos controles y planes de contingencia, o mejoras a los ya existentes, para evaluación de la Junta Directiva.

Diligenciamiento de las Matrices de Riesgo Operativo:

Las Matrices de Riesgo Operativo deberán contener por lo menos los siguientes campos:

Código Macroproceso a Evaluar
Código del Proceso
Código del Subproceso
Código Factor de Riesgo
Código Categoría de Riesgo
Código Subcategoría de Riesgo
Código del evento de pérdida
Descripción del evento de pérdida
Calificación de la probabilidad del riesgo inherente
Calificación del Impacto del riesgo inherente
Valuación del riesgo inherente
Descripción del cluster de control actual
Responsable del cluster de control actual
Calificación del diseño del cluster de control actual
Calificación de la efectividad del cluster de control actual

Esta información debe ser ingresada por cada funcionario de la Compañía, para los procesos en los que participa, y con la periodicidad establecida por el Comité de Riesgos, la cual debe ser por lo menos anual.

El Comité de Riesgos debe definir el medio o sistema a utilizar para que cada funcionario diligencie la Matriz de Riesgo Operativo. El medio o sistema utilizado debe permitir la consolidación de los resultados, a partir de los valores promedio de la información cuantitativa ingresada al sistema.

4.7. Riesgo Legal

De acuerdo con la Norma Externa de la Superintendencia Financiera, es la posibilidad de pérdida en que incurre una entidad al ser sancionada u obligada a indemnizar daños como resultado del incumplimiento de normas o regulaciones y obligaciones contractuales.

El riesgo surge también como consecuencia de fallas en los controles y transacciones, derivadas de actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos o transacciones.

4.8. Riesgo Reputacional

Según la Circular Externa 049 de 2006 de la Superintendencia Financiera, el riesgo reputacional se define como la posibilidad de pérdida en que incurre una entidad por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto a la institución y sus prácticas de negocios, que cause pérdida de clientes, disminución de ingresos o procesos judiciales.

También se puede definir como el conjunto de percepciones que tienen sobre la Compañía los diversos grupos de interés (Stakeholders) con los que se relaciona, tanto a nivel interno como externo. Esta reputación es el resultado del comportamiento desarrollado por la Compañía a lo largo del tiempo y describe su capacidad para distribuir valor a los mencionados grupos.

En su concepto más amplio, el Grupo de Interés (Stakeholders) incluyen a clientes, accionistas, empleados, directivos y al público en general, a quienes cualquier acción, hecho u operación de la Compañía pueda causarles un efecto.

4.8.1. Metodologías para monitorear y controlar el riesgo reputacional

Posición reputacional de la Compañía

Con el fin de analizar la posición reputacional de la Compañía, el modelo a seguir por parte de el Comité de Riesgos consiste en:

- a. Determinar el grado de percepción de los diferentes grupos de interés con respecto a las diferentes actividades realizadas por la Compañía.

Para ello, deben utilizarse herramientas como encuestas y entrevistas grupales a clientes, proveedores, medios de comunicación, etc., las cuales deben ser preparadas por el Comité de Riesgos y practicadas por el área respectiva que tenga contacto con el Grupo de Interés (Clientes, accionistas, empleados, directivos y público en general) que sea objeto de la encuesta o entrevista.

Estas encuestas o entrevistas deben hacerse en forma periódica, por lo menos una vez al año, de acuerdo con lo que determine la Junta Directiva .

Como resultado de las mismas, se pueden clasificar cada una de las actividades evaluadas, tanto de acuerdo con el tipo de Grupo de Interés que más percepción negativa mostró sobre dicha actividad (Medido como el porcentaje de los miembros de cada una de las clases de Grupos de Interés

que mostraron una percepción negativa acerca de la actividad analizada por medio de la encuesta o entrevista), como de acuerdo con el orden de percepción negativa de las actividades (Actividades con mayor porcentaje de Grupos de Interés que mostraron una percepción negativa acerca de la actividad analizada por medio de la encuesta o entrevista).

El Comité de Riesgos debe preparar un informe a la Junta Directiva con los respectivos resultados, denominado Informe de Posición Reputacional de la Compañía.

- b. La Gerencia de Riesgos debe además clasificar en el anterior informe las actividades de riesgo identificadas, de acuerdo con las siguientes cuatro situaciones:

Situación en la que la reputación de la actividad es buena y la realidad es mala. PLAN DE ACCION. Se requiere urgentemente tomar medidas al interior de la Compañía para ajustarse a dicha reputación y mitigar el riesgo reputacional.

Situación en la que la reputación de la actividad es mala y la realidad es mala. PLAN DE ACCION. Bajo estas circunstancias se debe tener en cuenta que cualquier intento por comunicar y publicitar a los Grupos de Interés algo que no se tiene, solo resulta contraproducente y termina por afectar más a la Compañía, por lo cual debe evitarse cualquier tipo de comunicación y publicidad al respecto.

Situación en la que la reputación de la actividad es buena y la realidad es buena. PLAN DE ACCION. Se debe aprovechar al máximo esta situación, comunicándola y publicitándola a todos los grupos de interés.

Situación en la que la reputación de la actividad es mala pero la realidad es buena. PLAN DE ACCION. En este caso se requiere de una rápida y fuerte labor de comunicación para capitalizar esta buena realidad.

En cualquiera de los cuatro casos anteriores, las medidas, incluyendo los planes de comunicación y publicidad respectivos, deben ser propuestos por las áreas de la Compañía que tienen a su cargo la respectiva actividad en conjunto con el Comité de Riesgos, para aprobación por parte la Junta Directiva.

El Comité de Riesgos, podrá ordenar a las diferentes áreas, la implementación y desarrollo de planes de acción específicos, con el fin de reducir o minimizar la exposición de la Compañía al riesgo reputacional.

4.9. Reporte de eventos de pérdida

Cada evento de pérdida individual ocurrido en la Compañía, debe ser reportado a el Comité de Riesgos independientemente de los seguros que se tengan contratados. Para ello, el Comité de Riesgos debe preparar un modelo de reporte donde se solicite a la persona que identificó la ocurrencia del evento, el diligenciar la información requerida según el Registro de eventos de riesgo operativo que se menciona más adelante.

El Comité de Riesgos, como administrador del Registro de eventos de riesgo operativo, debe asegurarse de que dicha información actualice inmediatamente el Registro.

Aquellas pérdidas con un valor individual mayor a diez millones de pesos (\$10.000.000), deberán ser informadas adicionalmente a la Junta Directiva, por intermedio de el Comité de Riesgos. Este umbral de Reporte podrá ser revisado y modificado por el Comité de Riesgos.

Aquellas pérdidas en las cuales no se pueda cuantificar su valor claramente, en el momento de su ocurrencia, y de la cual se estime que puede estar superando el umbral de reporte anteriormente establecido, se deberá dar aviso de la ocurrencia del mismo, estimando el valor de la pérdida, de acuerdo con los valores probables establecidos previamente en las Matrices de Riesgo Operativo. La cantidad concreta de pérdida en este último caso, deberá ser reportada cuanto antes, así como, entre tanto, variaciones que se consideren importantes en el valor inicialmente estimado.

En caso de aquellos eventos que pueden experimentar luego restituciones de valor, dichos valores restituidos también deben ser informados al Comité de Riesgos y a la Junta Directiva, de acuerdo con los límites antes señalados.

4.10. Niveles de aceptación del riesgo operativo

Los niveles de aceptación del riesgo operativo hacen referencia a la política que la Compañía adopte, basada en la cuantía de pérdida por la ocurrencia de un evento de pérdida y luego de implementados los controles necesarios para mitigarla, acerca de si está dispuesta a tolerar dicho cuantía o si prefiere trasladar el riesgo vía seguros.

Estos niveles de aceptación deben ser propuestos por el Comité de Riesgos, quien hace la respectiva validación antes de presentarlos a la Junta Directiva para su aprobación.

La Junta Directiva decidirá si transfiere, acepta o evita un riesgo, en los casos en que esto sea posible.

En el caso de optar por la contratación de un seguro, deben administrarse también los eventos de riesgo operativo asociados con dicho seguro.

4.11. Registro de eventos de riesgo operativo

El Comité de Riesgos es el responsable de elaborar y mantener actualizado un registro de eventos de riesgo operativo, de acuerdo con lo establecido por la Circular Externa 049/06 expedida por la Superintendencia Financiera.

Este registro debe contener todos los eventos de riesgo operativo ocurridos en la Compañía, bien sea que:

- Generan pérdidas y afectan el estado de resultados de la Compañía.
- Generan pérdidas y no afectan el estado de resultados de la Compañía.
- No generan pérdidas y por lo tanto no afectan el estado de resultados de la Compañía.

En estos últimos dos casos, la medición será de carácter cualitativo.

Este Registro debe tenerse en cuenta para la revelación contable que se menciona más adelante.

Cada área deberá proveer al Comité de Riesgos la información respectiva para diligenciar este Registro de eventos de riesgo operativo, de manera que el mismo contemple la totalidad de los eventos de riesgo operativo. El registro a cargo del Comité de Riesgo Operativo será el único aceptado.

Este registro deberá diligenciarse con, por lo menos, la siguiente información:

I. Referencia

Código interno, creado por el Comité de Riesgos, que relacione el evento en forma secuencial. Este código estará conformado por el subnumeral del respectivo evento, de acuerdo con lo establecido en el numeral 4.5. del presente Manual, seguido por la fecha de inicio del evento (Formato: Año,Mes,Día,Hora) y finalizando con un número de cinco dígitos, desde 00001 hasta 99999, que representa la secuencia de ocurrencia de dicho evento en particular.

II. Fecha de inicio del evento

Fecha en que se inicia el evento. Formato: Día, mes, año, hora.

III. Fecha de finalización del evento

Fecha en que finaliza el evento. Formato: Día, mes, año, hora.

IV. Fecha del descubrimiento

Fecha en que se descubre el evento. Formato: Día, mes, año, hora.

V. Fecha de contabilización

Fecha en que se registra contablemente la pérdida por el evento. Formato: Día, mes, año, hora.

VI. Divisa

Moneda extranjera en la que se materializa el evento.

VII. Cuantía

Monto de dinero (moneda legal) a que asciende la pérdida, definida como la cuantificación económica de la ocurrencia de un evento de riesgo operativo, así como los gastos derivados de su atención.

VIII. Cuantía recuperada

Monto de dinero recuperado por acción directa de la Compañía, incluyendo las cuantías recuperadas por seguros.

IX. Cuantía recuperada por seguros

Monto de dinero recuperado por el cubrimiento a través de un seguro.

X. Clase de evento

Clase de evento, según la clasificación adoptada en numeral 4.5., sin tener en cuenta subclasificaciones.

XI. Producto/Servicio afectado

Nombre del producto o servicio afectado.

XII. Cuentas PUC afectadas

Cuentas del Plan Único de Cuentas (PUC) afectadas.

XIII. Proceso

Nombre del proceso afectado.

XIV. Tipo de pérdida

Tipo de pérdida, de acuerdo con la siguiente clasificación:

- a) Generan pérdidas y afectan el estado de resultados de la Compañía.
- b) Generan pérdidas y no afectan el estado de resultados de la Compañía.
- c) No generan pérdidas y por lo tanto no afectan el estado de resultados de la Compañía.

XV. Descripción del evento

Descripción detallada del evento:

- Canal de servicio o atención al cliente (Cuando aplique)
- Zona geográfica

XVI. Líneas operativas

Identificación según clasificación suministrada por la Superintendencia Financiera de Colombia.

El Comité de Riesgos podrá, por decisión propia o a solicitud de la Junta Directiva incluir información adicional dentro de dicho Registro.

Con una periodicidad al menos semestral, el Comité de Riesgos debe preparar un informe a la Junta Directiva, sobre de Eventos de Pérdida, donde se organice la anterior información por frecuencia de ocurrencia y por magnitud del siniestro.

El Comité de Riesgos deberá estar atento a proponer los controles necesarios para aminorar la frecuencia de ocurrencia de aquellos riesgos que presenten la mayor cuantía histórica de siniestros, tomando una serie histórica de por lo menos tres años o la que exista en el Registro de eventos en ese momento, si es menor.

La Junta Directiva deberá aprobar los controles que considere necesarios, a partir de los propuestos por el Comité de Riesgos y gestionar obtención de los recursos necesarios para implementar dichos controles.

4.11.1. Metodología y procedimiento para implementar y mantener el Registro de eventos de Riesgo Operativo

METODOLOGIA:

La metodología establecida consiste en la participación activa de todos los funcionarios de la organización, desde sus respectivos cargos, en la identificación y reporte de los eventos de pérdida que ocurran en los procesos a su cargo, para que el Comité de Riesgos se encargue de consolidarlos en un sistema que permita construir una base de datos histórica, que se pueda consultar y permita su agrupación por diferentes criterios, con el fin de evaluar en cualquier momento el comportamiento histórico de los eventos de pérdida ocurridos en la Compañía.

PROCEDIMIENTO:

Paso 1: Cada funcionario debe conocer los posibles eventos de pérdida identificados en la Matriz de Riesgo de la Compañía y debe haber sido capacitado en el tema de qué es riesgo operativo y cuales son los factores y clases de eventos de pérdida establecidos por la Superintendencia Financiera.

En cada área, debe estar disponible tanto la definición de riesgo operativo y de cada factor y clase de evento de pérdida, como el listado de eventos identificados en la Matriz de Riesgos de la Compañía.

Paso2: Cuando algún funcionario observe una situación o hecho ocurrida en desarrollo de las actividades a su cargo o en desarrollo de los procesos en los cuáles el participa, y considera, con base en la capacitación previamente recibida, que estas situaciones o hechos pueden generar o han generado una pérdida para la Compañía, en el menor tiempo posible debe proceder a diligenciar el formato anexo a este Manual, el cuál estará disponible tanto en forma física como en hoja electrónica. En el primer caso, dentro de los formatos usados por cada área. En el segundo caso, en la carpeta designada por el Comité de Riesgos. En ambos casos, el formato cuenta con un instructivo de diligenciamiento.

En cualquier caso, el diligenciamiento del formato deberá realizarse a más tardar, dentro de las veinticuatro horas siguientes al momento en que el funcionario se ha dado cuenta de la ocurrencia del hecho o situación. En caso contrario, se tomará como falta grave el no informar a tiempo de lo anterior.

Paso 3: Una vez diligenciado el formato, el mismo debe ser enviado a el Comité de Riesgos, físicamente o por correo electrónico, para que la misma proceda a incluirlo en la base de datos denominada: Registro de Eventos de Riesgo Operativo. Copia del formato deberá ser entregada a la Auditoría Interna.

Paso 4: El funcionario del Comité de Riesgos, encargado de dicha actividad, procederá a incluir la información suministrada por cada funcionario, dentro de la base de datos creada para tal fin.

Paso 5: La Auditoría interna deberá incluir dentro de sus programas de revisión periódica, pruebas de verificación para confirmar que todos los eventos identificados por los diferentes funcionarios de la Compañía han sido incluidos dentro de la base de datos.

Paso 6: Por lo menos con una periodicidad mensual, el Comité de Riesgos generará un back up de la información contenida en la base de datos, de acuerdo con las condiciones mínimas para estos procesos, establecidos dentro de la entidad.

Paso 7: Mensualmente, el Comité de Riesgos generará un informe en donde se clasifiquen los eventos de pérdida identificados, de acuerdo con el área, factor de riesgo, clase de evento de pérdida y cualquier otro criterio que el Comité de Riesgos considere importante. Dicho informe será presentado en el Comité de Riesgos.

Paso 8: El Comité de Riesgos podrá citar a sus reuniones, a cualquier funcionario de las diferentes áreas, para analizar en conjunto o solicitar aclaraciones sobre el comportamiento de los eventos de pérdida ocurridos en los procesos de dichas áreas. Como resultado, el Comité de Riesgos podrá solicitar a los responsables de cada área, el desarrollo e implementación de controles y planes de contingencia para aminorar su riesgo operativo.

4.12. Procedimientos para el monitoreo y control del riesgo operativo

El monitoreo y control del riesgo operativo se basa en elementos como alertas tempranas, desarrollo de indicadores de gestión, controles y procesos para administrar la continuidad del negocio.

A continuación se describen dichos elementos:

4.12.1. Alertas tempranas

El Modelo de Alertas Tempranas que debe utilizar el Comité de Riesgos consiste en lo siguiente:

- a. En primer lugar, el Comité de Riesgos debe consolidar trimestralmente el valor del conjunto de eventos de pérdida de toda la Compañía, mediante la suma del Rating de Riesgo Inherente de todos los eventos de pérdida contemplados en la Matriz de Riesgo Operativo.

Este resultado se debe comparar con el patrimonio de la Compañía. En la medida en que el mismo aumente de un periodo a otro en forma tal que su participación dentro del patrimonio aumente en más de un determinado

porcentaje, el cual será establecido por el Comité de Riesgos, se configurará una alerta temprana que debe ser informada a la Junta Directiva, para su análisis y determinar las estrategias a seguir con el fin de controlar el riesgo operativo.

b. A partir de la actualización periódica de las Matrices de Riesgo Operativo (ORM), el Comité de Riesgos debe elaborar un informe donde se observe la evolución histórica, para cada evento de pérdida, de los siguientes aspectos:

- Impacto del riesgo inherente
- Frecuencia del riesgo inherente
- Diseño del cluster de control
- Efectividad del cluster de control

Aquellas tendencias que muestren un deterioro significativo en los controles o un aumento significativo en el valor de pérdida esperado, deberán ser objeto de informe al Comité de Riesgos para definir nuevos controles o planes de contingencia.

Se considera significativo, un comportamiento de un evento de pérdida en particular, cuya impacto y/o frecuencia de ocurrencia aumente por encima del promedio más una desviación estándar con respecto al valor del conjunto de eventos de pérdida de toda la Compañía, agregación que realiza el Comité de Riesgos a partir de la Matriz de Riesgo Operativo.

c. A partir del Registro de Eventos de Riesgo Operativo, se deben ordenar los eventos de pérdida por frecuencia de ocurrencia y por cuantía, de manera que aquellos que tengan la combinación más alta de estos dos elementos (Resultado de multiplicarlos), deben ser prioridad en la presentación de los planes de acción que el Comité de Riesgos o las diferentes áreas de la Compañía propongan a la Junta Directiva, haciendo alusión a este hecho.

4.12.2 Indicadores de Gestión

Estos indicadores, que deben ser calculados e informados por el Comité de Riesgos a la Junta Directiva, corresponden a fórmulas que reflejen si el control de riesgos y los planes de contingencia son adecuados o no.

Dicho de otra forma, son valores o fórmulas matemáticas que reflejen la evolución de un evento de riesgo; es decir, de una situación que de presentarse, generaría pérdidas para la Compañía.

El indicador debe evolucionar de forma tal que la exposición al riesgo se reduzca. Por ejemplo, un indicador puede ser el valor o número de cheques extraviados de la tesorería en un año. En la medida en que este valor del número de cheques se

reduzca a través del tiempo, menos expuesta está a la Compañía a pérdidas por esta razón y significa que los controles establecidos para evitar que se pierdan cheques y los planes de contingencia implementados para el caso de que un cheque se extravíe, funcionan adecuadamente.

Si un indicador de gestión refleja un comportamiento negativo, esto significa que el Comité de Riesgos debe estudiar nuevos controles o planes de contingencia para el respectivo proceso.

Entre otros ejemplos de indicadores, se mencionan los siguientes:

- Frecuencia de ocurrencia de eventos de pérdida por proceso. En la medida en que el valor de este indicador se reduzca, significa una mejor gestión.
- Impacto de los eventos de pérdida que han ocurrido por proceso. En la medida en que el valor de este indicador se reduzca, significa una mejor gestión.
- Evaluación de las capacitaciones en SARO y gestión de riesgos. En la medida en que el valor de este indicador sea mayor, significa una mejor gestión.
- Número de procesos con planes de contingencia. En la medida en que el valor de este indicador sea mayor, significa una mejor gestión.

Es importante que los indicadores de gestión hagan parte del sistema de evaluación del desempeño de los funcionarios y áreas de la Compañía, en lo que respecta a los procesos a su cargo.

El Comité de Riesgos será la instancia que proponga los mecanismos concretos a incluir en el sistema de evaluación de desempeño.

4.12.3. Controles

Además de la labor que el Comité de Riesgos tiene, de proponer nuevos controles para los eventos de pérdida identificados en la Matriz de Riesgo Operativo, buscando mejorar la calificación de su diseño y de su efectividad, el Comité de Riesgos debe evaluar la consistencia de los controles con respecto al evento de pérdida que buscan mitigar.

Para ello, debe evaluarse que el control tenga una magnitud acorde con el riesgo inherente. De manera que aquellos riesgos inherentes de mayor impacto y frecuencia de ocurrencia, deben tener cluster de control más completos.

Así mismo, pueden identificarse controles que son demasiado grandes, en términos de complejidad en su aplicación y costo, vinculados a riesgos inherentes de impacto y frecuencia muy bajos. En este caso, se debe revisar la posibilidad de ajustar dichos controles.

El Comité de Riesgos, deberá además revisar ocasionalmente los controles, mediante trabajo de campo donde se observe al funcionario encargado del control y la forma como lo aplica, para conceptuar si el control es insuficiente, si es necesario reforzarlo o si es necesario establecer otro control. Esta evaluación debe estar debidamente soportada para entregar un informe al respecto a la Junta Directiva.

En caso de que en el informe del Comité de Riesgos se exprese la urgencia de colocar algún control en particular en forma inmediata, el área involucrada debe proceder a suministrar los recursos para hacerlo, con el fin de no esperar hasta la reunión de la Junta Directiva.

4.12.4. Nuevos procesos o modificación de procesos existentes

Como requisito para que en cualquier área de la Compañía se modifique o implemente un nuevo proceso, el mismo debe ser objeto del análisis anterior de talleres o reuniones de trabajo, para evaluar el riesgo inherente y los controles que se deben implementar, con el objeto de que por intermedio del Comité de Riesgos, se presente a la Junta Directiva el informe respectivo.

Ningún proceso podrá iniciarse o modificarse sin que previamente se diseñe el cluster de control del mismo, aprobado por el Comité de Riesgos. Esto aplica también para la realización de operaciones de fusión, adquisición, cesión de activos, pasivos y contratos, entre otros.

4.12.5. Procesos para administrar la continuidad del negocio

En cumplimiento de la Circular Externa 049/06, la Compañía, teniendo en cuenta su estructura, tamaño, objeto social y actividades de apoyo, ha desarrollado un sistema de administración de la Continuidad del Negocio (BCM por sus siglas en inglés) el cual incluye los procesos de definir, implementar, probar y mantener dicho sistema en aspectos como: prevención y atención de emergencias, administración de la crisis, planes de contingencia y capacidad de retorno a la operación normal.

Los planes de continuidad del negocio deben cumplir, como mínimo, con los siguientes requisitos:

- a. Haber superado las pruebas necesarias para confirmar su eficacia y eficiencia.
- b. Ser conocidos por todos los interesados.

- c. Cubrir por lo menos los siguientes aspectos: identificación de eventos que pueden afectar la operación, actividades a realizar cuando se presentan fallas, alternativas de operación y regreso a la actividad normal.

4.11.6. Gobierno Corporativo

La Compañía debe contar con un Manual de Gobierno Corporativo, en donde se establezcan claramente las políticas en las relaciones con los diferentes grupos de interés.

Este Manual debe ser aprobado por la Junta Directiva de la Compañía.

4.12.7. Cultura de riesgos

Dentro de los planes de capacitación periódicos sobre gestión de riesgos operativos para todos los funcionarios de la Compañía, contemplados en el Manual de Administración del Riesgo Operativo, se debe resaltar la labor que cada funcionario tiene en la identificación de los factores de riesgo y eventos de pérdida en materia reputacional.

Adicionalmente, debe promoverse la identificación y control de factores generadores de riesgos, como una actividad propia de cada cargo al momento de evaluar desempeños.

Los indicadores de gestión de las diferentes áreas y funcionarios de la Compañía, deben incluir en lo posible aspectos relacionados con la gestión en la identificación y control de riesgos reputacionales. Estos indicadores deben medir además, por proceso, la evolución del impacto y frecuencia de los eventos de pérdida por proceso y la evolución del rating del Cluster de Control, en términos de su diseño y efectividad.

Estos indicadores deben ser elaborados por el Comité de Riesgos y presentados a la Junta Directiva, para su aprobación e implementación.

4.12.8. Coordinación de comunicaciones

La comunicación formal es la base para el correcto flujo de la información que se quiere hacer llegar a los diferentes Grupos de Interés, tanto internos como externos.

Por ello, toda información que se quiera transmitir debe hacerse a través de los canales establecidos para tal fin, de manera que no se considere válida ninguna otra información canalizada a través de otros medios.

Esto implica desestimular los canales no formales de comunicación, mediante el desarrollo de canales formales que tengan definidos claramente aspectos como responsables, forma de acceso a los mismos y periodicidad.

4.12.9. Canales de modificaciones de condiciones claros entre la Compañía y sus empleados y/o Clientes

Tanto los funcionarios de la Compañía como sus clientes deben conocer claramente el procedimiento por medio del cual se realizan cambios o modificaciones a las condiciones inicialmente pactadas entre ellos y la Compañía, como por ejemplo: promociones laborales o llamados de atención, en el caso de empleados, o cambio de planes o incremento en el costo de los mismos, en el caso de los clientes.

Para ello, se deben tener políticas y procedimientos claros establecidos al respecto, y ser comunicados mediante los canales formales adecuados.

4.12.10. Planes de Contingencia

Los planes de contingencia para la administración del riesgo reputacional, deben contemplar por lo menos lo siguiente:

a. Responsabilidades del Comité de Riesgos:

En caso de que alguna de las decisiones cuya responsabilidad es del Comité de Riesgos no pueda tomarse debido a la imposibilidad de reunir a dicho Comité, aquellas decisiones que a juicio de la Gerencia General revistan el carácter de urgentes, podrán ser aprobadas por dos miembros de la Junta Directiva, consultados telefónicamente.

El Comité de Riesgos deberá enviar un memorando escrito del Comité de Auditoría, donde se informe los elementos que tuvo en cuenta para considerar el carácter de Urgencia de la decisión y la decisión tomada.

b. Responsabilidades del Comité de Riesgos:

La persona encargada de tomar decisiones a cargo del Comité de Riesgos, en ausencia de la Gerente General, será el funcionario que formalmente quede encargado de la Gerencia, quien debe conocer el funcionamiento de los modelos de administración de riesgos, de acuerdo con lo establecido en el siguiente párrafo.

Los modelos de análisis, medición, seguimiento y control a los diferentes riesgos deben estar debidamente documentados. La Gerencia General y por lo menos

dos funcionarios del área deben conocer su forma de funcionamiento, para lo cual se deben programar capacitaciones periódicas de actualización en los mismos.

En caso de ausencia de un funcionario, las labores a su cargo deberán ser desarrolladas por el funcionario alterno que conozca los modelos, o por el Gerente de Riesgos.

c. Aspectos no contemplados en el presente Manual:

Cualquier situación no esperada y no contemplada en el presente manual o en el Manual de Riesgo Operativo, debe ser objeto de un Plan de Contingencia preparado por el Comité de Riesgos y aprobado por La Junta Directiva.

4.12.11. Reportes internos y externos

Tanto los reportes internos y externos, como los documentos y registros que evidencien la operación efectiva del SARO, deben tener las características de integridad, oportunidad, confiabilidad y disponibilidad de la información allí contenida.

Los reportes periódicos que se deben elaborar son los siguientes:

Tipo de reporte:	Interno
Nombre del Reporte:	Informe de Perfil de Riesgo Residual
Contenido:	Valor consolidado del riesgo residual de la Compañía
Responsable:	Comité de Riesgos
Usuario:	Junta Directiva
Periodicidad:	Semestral
Oportunidad:	Primeros 15 días del siguiente semestre

Tipo de reporte:	Interno
Nombre del Reporte:	Informe de Gestión del Representante Legal
Contenido:	Debe incluir una indicación sobre la gestión adelantada en materia de administración del riesgo operativo.
Responsable:	Representante Legal
Usuario:	Asamblea de Accionistas
Periodicidad:	Al cierre de cada ejercicio contable
Oportunidad:	El plazo establecido para realizar la Asamblea de Accionistas

Tipo de reporte:	Interno
Nombre del Reporte:	Informe de Alertas Tempranas

Contenido: Indicadores que reflejen un aumento inusual en el nivel de riesgo de algún evento de pérdida.
Responsable: Comité de Riesgos
Usuario: Junta Directiva
Periodicidad: Semestral
Oportunidad: Primeros 15 días del siguiente semestre

Tipo de reporte: Interno
Nombre del Reporte: Matrices de Riesgo Operativo
Contenido: Resumen consolidado del riesgo inherente, cluster de control y riesgo residual.
Responsable: Comité de Riesgos
Usuario: Junta Directiva
Periodicidad: Semestral
Oportunidad: Primeros 15 días del siguiente semestre

Tipo de reporte: Externo
Nombre del Reporte: Informe de Gestión del Riesgo Operativo para el público en general
Contenido: Información sobre el volumen y el perfil de riesgo de las operaciones de la Compañía, con el fin de que el público pueda evaluar las estrategias de Gestión de Riesgo Operativo adoptadas por la Compañía.
Responsable: Comité de Riesgos
Usuario: Público en general a través de la internet
Periodicidad: Actualización anual
Oportunidad: Primeros tres meses de cada año

Informe de Identificación de Factores de Riesgo Reputacional: Este reporte es elaborado por el Comité de Riesgos y presentado a la Junta Directiva, con una periodicidad por lo menos semestral.

5. PLATAFORMA TECNOLÓGICA

El Comité de Riesgos debe evaluar periódicamente la tecnología y los sistemas utilizados para garantizar el adecuado funcionamiento del SARO, con el fin de verificar si se ajustan a las actividades y tamaño de la Compañía.

Un informe al respecto debe ser presentado a la Junta Directiva, con una periodicidad por lo menos anual.

6. REVELACION CONTABLE

De acuerdo con lo establecido en la Circular Externa 049/06 de la Superintendencia Financiera, los eventos de riesgo operativo, cuando no afecten el estado de resultados deben ser revelados en cuentas de orden, de acuerdo con la metodología para su cuantificación establecida por cada entidad.

Cuando dichas pérdidas afecten el estado de resultados, se registrarán en la cuenta del gasto determinada por la Superintendencia Financiera en el Plan Unico de Cuentas, para que dicho acontecimiento quede registrado en el periodo en el que se materializó la pérdida.

Además, en las notas a los Estados Financieros de la Compañía, se señalarán las causas que originaron los eventos de riesgo operativo, revelados en cuentas de orden o registradas en el estado de resultados.

7. CAPACITACION Y DIVULGACION

El Comité de Riesgos tendrá a su cargo el diseño, programación y coordinación del Plan Anual de capacitación en el SARO, dirigido a todas las áreas y funcionarios de la Compañía.

Los programas de capacitación deberán dictarse también a los nuevos funcionarios vinculados a la compañía, durante su primer mes luego de haber ingresado a la Compañía, así como a los terceros de los cuales se tenga una relación jurídica de prestación de servicios diferente a aquella que se origina en un contrato de trabajo, como el caso del outsourcing. Para el caso de estos terceros, la capacitación deberá darse con anterioridad a la firma del contrato u orden de servicios y como requisito del mismo.

El Comité de Riesgos será responsable de la revisión y actualización trimestral de dichos programas de capacitación. Adicionalmente, deberá desarrollar y aplicar las evaluaciones que se practicarán a los participantes en dichos programas, tanto en el momento inmediatamente posterior a la capacitación como posteriormente, por lo menos una vez al año a todos los funcionarios y terceros.

El Comité de Riesgos debe contar con los mecanismos de evaluación de los resultados obtenidos, con el fin de determinar la eficacia de dichos programas y el alcance de los objetivos propuestos.

8. Anexos

Anexo 1

DEFINICION DE TERMINOS

Back Testing: Pruebas efectuadas para verificar el adecuado funcionamiento de un modelo o para validar sus resultados.

Cluster de Control: Suma de controles y la clasificación a la que pertenecen.

Dueño del Proceso: Responsable de la administración de un proceso; es decir, de su planeación, organización, dirección y control.

Evento: Incidente o situación que ocurre en un lugar particular durante un intervalo de tiempo determinado.

Eventos de pérdida: Son aquellos incidentes que generan pérdidas por riesgo operativo a las entidades.

Facilitador: Persona que por su conocimiento de un proceso o de una labor, ayuda a orientar y aclarar las dudas de un grupo de trabajo, en donde se desarrollan actividades relacionadas con dicho proceso o labor.

Factores de riesgo: Son las fuentes generadoras de eventos en las que se originan las pérdidas por riesgo operativo. Son factores de riesgo el recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos.

Factores de riesgo externos: Son eventos asociados a la fuerza de la naturaleza u ocasionados por terceros, que escapan en cuanto a su causa y origen al control de la Compañía.

GAP: Brecha. En los términos del presente Manual, situación en la cual un evento de pérdida permanece sin clasificarse en ninguna de las categorías de riesgo existentes.

Gobierno Corporativo: Códigos de Buen Gobierno Corporativo que deben ajustarse a la actividad comercial de cada sociedad y arrojar como resultado un marco autorregulatorio que garantice a los clientes, accionistas y otros aportantes de recursos, transparencia, objetividad y competitividad.

IT: Información y Tecnología. Área especializada dentro de las empresas para desarrollar actividades relacionadas con este tema.

Índices multifactoriales: Índices que incluyen la evaluación de varios factores para poder analizar una variable.

Manual de Riesgo Operativo: Es el documento contentivo de todas las políticas, objetivos, estructura organizacional, estrategias, los procesos y procedimientos aplicables en el desarrollo, implementación y seguimiento del SARO.

Matrices de Riesgo: Bases de datos que contienen toda la información necesaria para identificar una clase de riesgo en particular, incluyendo sus características, los controles y planes de contingencia establecidos, y los responsables de los mismos. Estas Matrices también contiene una calificación o rating para cada riesgo o evento de pérdida.

Outsourcing: Servicio relacionado con actividades administrativas y/o operativas de la que la misma subcontrata con terceros en lugar de realizarlo ella misma.

Pérdidas: Cuantificación económica de la ocurrencia de un evento de riesgo operativo, así como los gastos derivados de su atención.

Perfil de Riesgo: Resultado consolidado de la medición de los riesgos a los que se ve expuesta una entidad.

Plan de continuidad del negocio: Conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retornar y continuar la operación, en caso de interrupción.

Plan de contingencia: Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.

Proceso: Conjunto interrelacionado de actividades para la transformación de elementos de entrada en productos o servicios, para satisfacer una necesidad, tanto interna como externa.

Rating: Clasificación

Riesgo inherente: Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo legal: Es la posibilidad de pérdida en que incurre una entidad al ser sancionada u obligada a indemnizar daños como resultado del incumplimiento de normas o regulaciones y obligaciones contractuales. El riesgo legal surge también como consecuencia de fallas en los contratos y transacciones, derivadas de actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos o transacciones.

Riesgo reputacional: Es la posibilidad de pérdida en que incurre la Compañía por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto de la institución y sus prácticas de negocios, que cause pérdida de clientes, disminución de ingresos o procesos judiciales.

Riesgo residual: Nivel resultante del riesgo después de aplicar los controles.

Impacto: Impacto de un evento en términos económicos o monetarios.

Sistema de Administración de Riesgo Operativo (SARO): Conjunto de elementos tales como políticas, procedimientos, documentación, estructura organizacional, registro de eventos de riesgo operativo, órganos de control, plataforma tecnológica, divulgación de información y capacitación, mediante los cuales las entidades vigiladas identifican, miden, controlan y monitorean el riesgo operativo.

Sobreposición: En los términos del presente Manual, situación en la cual un evento de pérdida se clasifica en más de una categoría de riesgo al tiempo, lo que da lugar a su doble conteo.

Solvencia: Es el respaldo marginal que deben poseer las empresas de seguros, para hacer frente a posibles situaciones de siniestralidad futura técnicamente no previstas y que se determina en función de parámetros establecidos por la Superintendencia.

Comité de Riesgos: Es el área o cargo, designada por el Representante Legal de la Compañía, la cual deberá coordinar la puesta en marcha y seguimiento del SARO.