MANUAL DE GESTIÓN DE RIESGO OPERACIONAL

Zumma Ratings S.A. de C.V. Clasificadora de Riesgo

SEGÚN LO ESTABLECIDO EN LAS NORMAS TÉCNICAS PARA LA GESTION INTEGRAL DE RIESGOS DE LAS ENTIDADES DE LOS MERCADOS BURSÁTILES - NRP-11

Código del Manual: PR-03
Versión: 002
Fecha de aprobación: 09/03/2026

INDICE

I. INTRODUCCIÓN

El presente Manual de Gestión del Riesgo Operacional establece el marco técnico, metodológico y normativo para la identificación, evaluación, control, mitigación, monitoreo y reporte del riesgo operacional al que se encuentra expuesta la Clasificadora de Riesgo, en cumplimiento de las Normas Técnicas para la Gestión Integral de Riesgos de las Entidades de los Mercados Bursátiles (NRP-11) emitidas por la Superintendencia del Sistema Financiero.

La gestión del riesgo operacional constituye un elemento esencial del sistema de control interno, permitiendo identificar y administrar los riesgos derivados de deficiencias en el recurso humano, procesos, tecnología, infraestructura o eventos externos, incluyendo el riesgo legal y reputacional asociados.

II. OBJETIVO

Establecer los lineamientos, políticas, metodologías y responsabilidades para la gestión integral del riesgo operacional, asegurando su adecuada identificación, evaluación, control, mitigación, monitoreo y reporte.

III. ALCANCE

El presente manual es de aplicación obligatoria para la Junta Directiva, Comité de Riesgos, Alta Gerencia, todas las áreas operativas, técnicas y administrativas, así como para terceros que participen en procesos críticos.

IV. MARCO NORMATIVO

La gestión del riesgo operacional se rige por las Normas Técnicas para la Gestión Integral de Riesgos de las Entidades de los Mercados Bursátiles (NRP-11), normativa emitida por la SSF, el Manual de Gestión Integral de Riesgos y demás disposiciones legales aplicables.

V. GOBIERNO CORPORATIVO DEL RIESGO OPERACIONAL

El gobierno del riesgo operacional constituye un pilar fundamental del sistema de gestión integral de riesgos de la Clasificadora y tiene como objetivo asegurar una adecuada supervisión, control y rendición de cuentas en la administración de este riesgo.

Junta Directiva: es responsable de aprobar las políticas, el apetito y la tolerancia al riesgo operacional, así como de supervisar periódicamente la exposición de la Entidad a este riesgo y la efectividad del sistema de control interno.

Comité de Riesgos: tiene a su cargo la supervisión continua de la gestión del riesgo operacional, la revisión del perfil de riesgo, el análisis de eventos relevantes y la recomendación de acciones correctivas a la Junta Directiva.

Unidad de Riesgos: es responsable de coordinar la implementación del sistema de gestión del riesgo operacional, desarrollar metodologías, mantener la matriz de riesgos, consolidar la información y elaborar los reportes correspondientes.

Dueños de proceso: son responsables de identificar, evaluar, controlar y mitigar los riesgos operacionales inherentes a sus procesos, así como de implementar y mantener los controles definidos.

Auditoría Interna: realiza evaluaciones independientes sobre la efectividad del sistema de gestión del riesgo y del control interno, informando sus resultados a la Junta Directiva y a los órganos de gobierno correspondientes.

VI. MARCO CONCEPTUAL DEL RIESGO OPERACIONAL

Se entiende por Riesgo Operacional la posibilidad de incurrir en pérdidas derivadas de deficiencias, fallas o inadecuaciones en el recurso humano, los procesos, los sistemas de información o acontecimientos externos, incluyendo el riesgo legal y reputacional asociados.

Características del Riesgo Operacional:

- Es transversal a todos los procesos
- Se origina sobre hechos reales
- Tiene efecto multiplicador sobre otros riesgos
- Su materialización puede ser inmediata y de impacto económico o no.

VII. FACTORES DE RIESGO

Los factores de riesgo operacional comprenden aquellas fuentes internas y externas que pueden dar origen a eventos de pérdida y afectar el normal desarrollo de las operaciones de la Clasificadora. En este sentido, los factores de riesgo operacional incluyen, sin limitarse a ellos, las personas, los procesos, los sistemas de información y los acontecimientos externos, de acuerdo con el detalle siguiente:

- **Personas:** se refiere a las personas vinculadas directa o indirectamente con la Entidad, cuya actuación, omisión, falta de capacitación, negligencia, errores involuntarios o conductas contrarias a las políticas internas pueden generar riesgos operacionales, legales o reputacionales.

- **Procesos:** comprenden el conjunto de actividades, procedimientos y flujos de trabajo que permiten la prestación de los servicios de la Clasificadora. Deficiencias en su diseño, documentación, ejecución, supervisión o actualización pueden dar lugar a errores operativos, incumplimientos normativos o fallas en la calidad del servicio.

- **Sistemas de Información**: incluye lo referente a tecnología, aplicaciones, infraestructura tecnológica, hardware, software y telecomunicaciones que soportan los procesos operativos y administrativos. Fallas, interrupciones, accesos no autorizados o deficiencias en la seguridad de la información pueden afectar la continuidad operativa y la confiabilidad de la información.

- **Acontecimientos externos:** corresponden a eventos ajenos al control de la Clasificadora, tales como desastres naturales, fallas en servicios públicos, actos de terceros, cambios regulatorios o situaciones de orden social, que puedan impactar directa o indirectamente sus operaciones.

Cada uno de estos factores de riesgo deberá ser identificado, evaluado, monitoreado y controlado mediante mecanismos formales, incluyendo la definición de responsables, la implementación de controles preventivos y correctivos, la utilización de indicadores clave de riesgo y el seguimiento periódico de su efectividad, en concordancia con el sistema de gestión integral de riesgos y el perfil de riesgo aprobado por la Junta Directiva.

VIII. CLASIFICACIÓN DE EVENTOS DE PÉRDIDA

Los eventos de pérdida corresponden a incidentes o situaciones que se materializan como consecuencia del riesgo operacional y que generan o pueden generar impactos negativos para la Clasificadora, ya sea de naturaleza financiera, legal, reputacional u operativa. Para efectos de su adecuada gestión, los eventos de pérdida se clasifican de acuerdo con su naturaleza y origen, conforme a lo establecido en la NRP-11 y a las mejores prácticas internacionales.

La Clasificadora adoptará la siguiente clasificación de eventos de pérdida:

1. **Fraude interno:** Actos intencionales realizados por empleados, directivos o administradores, que buscan defraudar, apropiarse indebidamente de activos, manipular información o incumplir normas internas o externas.
2. **Fraude externo:** Actos realizados por terceros ajenos a la Entidad, orientados a defraudar, apropiarse indebidamente de activos, vulnerar sistemas o afectar la información de la Clasificadora.
3. **Relaciones laborales:** Eventos derivados del incumplimiento de la legislación laboral, conflictos laborales, prácticas inadecuadas de gestión del personal o condiciones de trabajo que generen contingencias legales o reputacionales.
4. **Clientes:** Fallas negligentes o involuntarias en el cumplimiento de obligaciones profesionales frente a los clientes, incluyendo errores en la prestación del servicio, divulgación inadecuada de información o incumplimientos contractuales.

5. **Daños a activos físicos:** Pérdidas ocasionadas por daños, deterioro o destrucción de activos físicos de la Entidad, como resultado de accidentes, desastres naturales o actos de terceros.

6. **Fallas tecnológicas:** Pérdidas derivadas de interrupciones, fallas o deficiencias en los sistemas de información, infraestructura tecnológica o seguridad de la información.

7. **Ejecución y administración de procesos:** Pérdidas originadas por errores en la ejecución de los procesos, deficiencias en los controles, fallas en la documentación o incumplimiento de procedimientos establecidos.

El reporte de eventos de riesgo operacional debe ser presentado ante la SSF anualmente, sin embargo, la entidad deberá informar a la SSF en un plazo máximo de tres días hábiles al tener conocimiento de cualquier aspecto relacionado con la exposición de riesgos, que puedan impactar en forma cualitativa o cuantitativa a la entidad.

IX. EVALUACIÓN DEL RIESGO OPERACIONAL

1. Metodología de Evaluación

La evaluación del riesgo operacional se desarrollará bajo las siguientes etapas:

- Identificación del riesgo
- Medición y determinación del riesgo inherente
- Evaluación de controles
- Determinación del riesgo residual
- Definición de acciones de mitigación
- Monitoreo y reporte

2. Identificación de Riesgos

La identificación de los riesgos operacionales se realizará de forma sistemática y periódica, abarcando todos los procesos misionales, operativos y de apoyo de la Clasificadora.

La identificación de riesgos deberá documentarse adecuadamente, estableciendo su causa, evento y posible impacto, y será revisada de manera continua para incorporar cambios en el entorno interno o externo.

Para tal efecto, se utilizarán herramientas tales como mapas de procesos, matrices de riesgo, análisis de eventos históricos, revisiones de auditoría, autoevaluaciones de riesgo y control,

así como evaluaciones periódicas realizadas por los dueños de proceso y la Unidad de Riesgos.

3. Medición y Evaluación

Los riesgos operacionales identificados serán evaluados considerando criterios de probabilidad de ocurrencia e impacto potencial, los cuales podrán incluir impactos financieros, operativos, legales, regulatorios y reputacionales.

La evaluación permitirá determinar el riesgo inherente, así como el riesgo residual, una vez considerados los controles existentes. Los niveles de riesgo resultantes serán clasificados conforme la matriz institucional, permitiendo su priorización y gestión de acuerdo con el apetito y tolerancia definidos por la Junta Directiva.

4. Control y Mitigación

Para cada riesgo identificado la Clasificadora analizará los controles existentes, orientados a reducir la probabilidad de ocurrencia y/o el impacto de los riesgos operacionales. Dichos controles podrán ser de carácter preventivo, detectivo o correctivo**,** y deberán estar debidamente documentados y asignados a responsables específicos.

Asimismo, se definirán planes de acción para aquellos riesgos cuyo nivel residual exceda los límites de tolerancia establecidos, los cuales deberán incluir acciones concretas, responsables y plazos de ejecución, y serán objeto de seguimiento periódico.

5. Monitoreo y Reporte

El riesgo operacional será monitoreado de forma continua mediante indicadores clave de riesgo (KRI), seguimiento de eventos de pérdida y evaluaciones periódicas del perfil de riesgo operacional.

La Unidad de Riesgos elaborará reportes periódicos dirigidos al Comité de Riesgos y a la Junta Directiva, los cuales incluirán información sobre la evolución del riesgo operacional, eventos relevantes, efectividad de los controles y estado de los planes de mitigación. Los eventos significativos deberán ser reportados de manera inmediata a los órganos de gobierno correspondientes.

6. Apetito y Tolerancia al Riesgo Operacional

La Clasificadora adopta un apetito de riesgo operacional bajo, considerando:

- La naturaleza técnica de su actividad
- Su rol en el mercado financiero
- La relevancia de su credibilidad e independencia

- La importancia de preservar la continuidad operativa

El apetito y la tolerancia son definidos y aprobados por la Junta Directiva, estableciendo límites cuantitativos y cualitativos que determinan el nivel máximo de exposición aceptable.

X. GESTIÓN DE EVENTOS DE PÉRDIDA

Todos los eventos de pérdida deberán ser registrados en una base de datos centralizada, incluyendo información sobre su naturaleza, causa, impacto, área afectada y acciones correctivas implementadas.

La información recopilada será utilizada para el análisis de causas raíz, la identificación de tendencias y la mejora continua del sistema de gestión del riesgo operacional, contribuyendo al fortalecimiento del control interno y la prevención de eventos futuros.

XI. INTEGRACIÓN CON OTROS RIESGOS

La gestión del riesgo operacional se realizará de manera integrada con los riesgos legal, reputacional, tecnológico y de continuidad del negocio, reconociendo que estos riesgos se encuentran interrelacionados y pueden potenciarse entre sí.

Esta integración permitirá una visión holística del perfil de riesgo de la Clasificadora y facilitará la adopción de medidas coordinadas para su adecuada administración, en concordancia con el sistema de gestión integral de riesgos.

XII. CULTURA Y CAPACITACIÓN

La Clasificadora promoverá una cultura organizacional orientada a la prevención, control y gestión del riesgo operacional, mediante programas de capacitación continúa dirigidos a todos los niveles de la Entidad.

Dichos programas buscarán fortalecer la conciencia del personal respecto a su rol en la gestión del riesgo operacional, fomentar el cumplimiento de las políticas y procedimientos establecidos y promover la comunicación oportuna de eventos e incidencias, contribuyendo así a la mejora continua del sistema de gestión.

XIII. REVISIÓN Y ACTUALIZACIÓN DEL MANUAL

El presente Manual será revisado y/o actualizado al menos una vez al año o cuando ocurran cambios regulatorios, estratégicos o eventos relevantes que lo ameriten.

En conjunto con la Dirección, la Unidad de Riesgos hará las modificaciones necesarias para someterlas a revisión del Comité de Riesgos y posteriormente a aprobación de la Junta Directiva e informar a la SSF, a fin de proceder posteriormente, a su difusión, implementación y actualización periódica.

XIV. VIGENCIA

El presente Manual entra en vigencia a partir de su aprobación por la Junta Directiva y es de cumplimiento obligatorio para toda la organización.

Elaboración y Revisión del documento

Acción	Versión	Fecha	Aprobación
Elaboración	Versión 1	31/01/2017	Junta Directiva – Acta No. 36
Modificación	Versión 2	09/03/2026	Junta Directiva – Acta No. 134

Modificación aprobada

En Sesión de Junta Directiva, de acuerdo con Acta No. 134 de fecha 09 de marzo 2026.

NOTA CONFIDENCIAL: Este Manual de Gestión de Riesgo Operacional es propiedad exclusiva y confidencial de Zumma Ratings S.A. de C.V. Clasificadora de Riesgo. Contiene información sensible y propietaria cuya divulgación no autorizada está estrictamente prohibida y podría perjudicar gravemente a la empresa. Al acceder a este Manual, usted se compromete a mantener su contenido en la más estricta confidencialidad, utilizarlo únicamente para los fines autorizados y a no divulgarlo, reproducirlo o compartirlo con terceros no autorizados. Las obligaciones de confidencialidad persisten indefinidamente, incluso después de finalizar su relación con la empresa y el incumplimiento de estos términos puede acarrear consecuencias legales y contractuales.