



Política de Gobierno Corporativo y Riesgo Operacional

Vantrust Capital

Septiembre 2026

Contenido

1. Control de cambios	4
2. Historial de Modificaciones	4
3. Objetivo.....	5
4. Alcance	5
5. Vigencia	5
6. Modelo de Gestión de Riesgo	5
6.1. Primera línea de defensa. Áreas de negocio y de apoyo.	6
6.2. Segunda línea de defensa.	6
6.3. Tercera línea de defensa. Auditoría Interna.....	6
7. Definiciones y Documentos Relacionados	6
7.1. Riesgo de Crédito	6
7.2. Riesgo de Mercado	7
7.3. Riesgo Liquidez	7
7.4. Riesgo LA/FT/FP	7
7.5. Riesgo Operacional	7
7.6. Riesgo Tecnológico	8
7.7. Riesgo Externalización de Servicios.....	8
7.8. Riesgo de Conducta	8
8. Gobierno Corporativo	9
9. Política de Gestión de Riesgo Operacional.....	9
9.1. Identificación del Riesgo Operacional	9
9.2. Análisis y Evaluación de Riesgo.....	10
9.3. Identificación de Controles y Mitigantes	10
9.4. Evaluación del Riesgo Residual.....	10
9.5. Apetito de Riesgo, Tolerancia y Tratamiento	11
9.6. Actividades de Seguimiento y Monitoreo	12
10. Matriz de Riesgo.....	12
11. Eventos de Riesgo Operacional y Base de Pérdidas	13
12. Testeo de Controles	13
13. Plan de Gestión de Riesgo Operacional	13
14. Capacitación	14

15. Roles y Responsabilidades.....	14
15.1. Directorio.....	14
15.2. Comité de Riesgo Operacional.....	14
15.3. Gerente General.....	15
15.4. Área de Riesgo Operacional.....	15
15.5. Área de Negocio	15
15.6. Auditoría Interna	15
16. Excepciones	16

1. Control de cambios

Versión	Fecha	Revisión	Comentario	Aprobación	
				Comité	Directorio
V 1.0	Jul 2025	Gerente Compliance y RO / Jefe Riesgo Operacional	Creación Documento	Ago 2025	Sep 2025
V 2.0	Sep 2026		Preparado Jefe Riesgo Operacional	Sep 2026	Sep 2026

2. Historial de Modificaciones

Rev. N°	Identificación de la modificación	Fecha
1	Creación de documento	11-09-2025
2	Incorpora responsabilidades de área de Auditoría Interna y complementa responsabilidades del Directorio, Modelo de gestión de riesgo, precisiones en objetivo, alcance y se incorporan definiciones de riesgo y referencia a política correspondiente.	09-09-2026

3. Objetivo

La presente Política reúne los lineamientos y definiciones que Vantrust Capital aplica para la gestión de riesgos y el control interno, en línea con la normativa vigente de la Comisión para el Mercado Financiero. Su propósito es dotar a la organización de una forma clara y metódica de identificar, medir, evaluar, tratar y monitorear los riesgos a los que se expone, dando seguimiento a las medidas de mitigación hasta su implementación.

Esta Política aplica a las entidades del Grupo Vantrust reguladas por la CMF la Administradora General de Fondos (AGF), con la NCG N°507 de 2024 y su modificatoria NCG N°527 de 2024 (gobierno corporativo y gestión integral de riesgos, AGF); y la Corredora de Bolsa (CdB) con la NCG N°528 de 2024 (gobierno corporativo y gestión integral de riesgos, CdB). Además de la NCG N°510 de 2024 sobre gestión de riesgo operacional, modificada por la NCG N°529 de 2024 (a su vez modificada por la NCG N°531 de 2025).

4. Alcance

Esta Política aplica a todos los colaboradores de las entidades del Grupo Vantrust Capital reguladas por la Comisión para el Mercado, incluyendo a los miembros de sus Directorios y al personal externo o contratistas que accedan a sus activos de información. Las obligaciones relativas a la externalización de servicios alcanzan además a los proveedores, en los términos que establezcan los respectivos contratos.

La gestión contenida en esta Política abarca el riesgo operacional y sus ámbitos: continuidad de negocio, externalización de servicios, y seguridad de la información y ciberseguridad. Los demás riesgos de la entidad (crédito, mercado, liquidez y de lavado de activos, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva) se gestionan conforme a sus políticas específicas y se consolidan en la matriz integral de riesgos.

Toda mención contenida dentro de esta política que hace alusión al “Directorio de Vantrust Capital”, “Directorio de Vantrust” o solamente “Directorio”, se hace extensivo a todos los Directorios de las empresas del Grupo Vantrust. Igual criterio aplica a las referencias al Comité de Riesgo Operacional, la Gerencia General y el área de Riesgo Operacional.

5. Vigencia

La presente Política se revisará y actualizará anualmente por el Directorio o, producto de cambios relevantes dentro de los procesos de negocio o normativa vigente.

6. Modelo de Gestión de Riesgo

La gestión del riesgo de la entidad se estructura conforme al modelo de tres líneas de defensa, que distribuye responsabilidades diferenciadas y asegura la independencia entre quienes asumen el riesgo, quienes lo supervisan y quienes lo auditan.

6.1. Primera línea de defensa. Áreas de negocio y de apoyo.

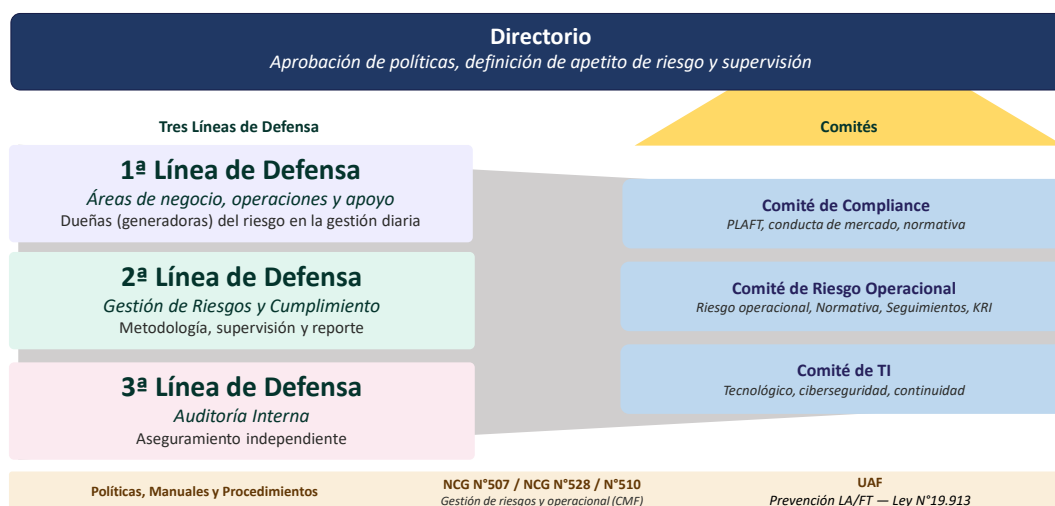
Son las dueñas del riesgo en sus procesos de negocio. Corresponde identificar, gestionar y controlar los riesgos operacionales inherentes a sus actividades diarias, aplicar los controles definidos y reportar oportunamente los eventos de riesgo operacional.

6.2. Segunda línea de defensa.

Es una función independiente de las áreas generadoras de riesgo. Corresponde definir la metodología de gestión de riesgo, mantener una matriz de riesgo, cuestionar y validar la gestión de la primera línea, monitorear los indicadores clave de riesgo (KRI), administrar la base de eventos y pérdidas operacionales de forma integral, reportar al Comité de Riesgo Operacional y al Directorio.

6.3. Tercera línea de defensa. Auditoría Interna.

Es una función independiente de las áreas de negocio y de la función de gestión de riesgos, con reporte directo al Directorio. Corresponde proveer aseguramiento independiente sobre la efectividad del sistema de control interno y de la gestión de riesgos, evaluando el desempeño tanto de la primera como de la segunda línea de defensa.



7. Definiciones y Documentos Relacionados

7.1. Riesgo de Crédito

Exposición a pérdidas económicas derivadas del incumplimiento, por parte de un tercero, de los términos y condiciones estipulados en un contrato, convenio u otro acto jurídico. Se puede descomponer según lo siguiente:

- **Riesgo de contraparte:** Exposición a pérdidas por el incumplimiento de la contraparte de sus obligaciones en una transacción financiera.

- **Riesgo crediticio del emisor:** Exposición a pérdidas por el deterioro de la solvencia, la quiebra o el sometimiento a un procedimiento concursal del emisor de instrumentos financieros mantenidos en cartera.

Los lineamientos y gestión de Riesgo de Crédito quedan acotados en la **Política de Riesgo de Crédito**.

7.2. Riesgo de Mercado

Exposición a pérdidas por variaciones en los precios de mercado que puedan afectar adversamente la situación financiera de la cartera propia de la entidad o de las carteras de terceros que administra. Comprende el riesgo de tasas de interés, el riesgo cambiario y el riesgo de precios asociados a los activos financieros de dichas carteras.

7.3. Riesgo Liquidez

Exposición de la entidad o de las carteras que administra a una potencial pérdida derivada de la necesidad de obtener fondos de manera inmediata para cumplir sus compromisos financieros.

- **Riesgo de liquidez de financiamiento:** Exposición a una pérdida potencial por la incapacidad de obtener recursos, conseguir o refinanciar préstamos a una tasa conveniente, o cumplir con las exigencias de los flujos de caja proyectados.
- **Riesgo de liquidez de mercado:** Exposición a una pérdida potencial por la incapacidad de liquidar un activo en cartera sin afectar adversamente su precio, dada la escasa profundidad del mercado de ese activo.

Para la Administradora General de Fondos, los lineamientos y gestión de liquidez quedan acotados en la **Política de Liquidez**.

7.4. Riesgo LA/FT/FP

Posibilidad de pérdida o daño que puede sufrir la entidad por su propensión a ser utilizada como instrumento para la canalización de recursos hacia actividades terroristas o el financiamiento de armas de destrucción masiva, o para ocultar o disfrazar el origen ilícito de bienes o recursos provenientes de actividades delictivas.

Los lineamientos y gestión de riesgo de LA/FT/FP se encuentran contenidos en la **Política y Procedimiento de Prevención de Delitos**.

7.5. Riesgo Operacional

Riesgo de que las deficiencias en los sistemas de información, los procesos internos o el personal, o las perturbaciones ocasionadas por acontecimientos externos, provoquen la reducción, el deterioro o la interrupción de los servicios que presta la entidad y, eventualmente, originen pérdidas financieras.

La presente política en su segunda parte entrega los lineamientos y herramientas para la gestión.

7.6. Riesgo Tecnológico

Riesgo de pérdidas derivadas de fallas, deficiencias o interrupciones en los sistemas de información y en la infraestructura tecnológica, incluyendo la continuidad de negocio, seguridad de la información y la ciberseguridad.

Sus lineamientos y gestión se documentan en el **Manual de Políticas de Seguridad de la Información**.

7.7. Riesgo Externalización de Servicios

Exposición a pérdidas derivadas de deficiencias o fallas en la provisión, por parte de terceros, de servicios contratados por la entidad, cuando ello afecte el cumplimiento normativo, la continuidad del negocio, la seguridad de la información o la calidad de sus servicios, productos, información e imagen.

Los lineamientos y gestión quedan supeditada a lo documentado en la **Política de Gestión de Riesgo de Proveedores**.

7.8. Riesgo de Conducta

Riesgo asociado al cumplimiento de cinco principios en la relación con los clientes: i) trato justo a los clientes de entidades financieras; ii) adecuada gestión de conflictos de interés; iii) protección de la información de los clientes; iv) transparencia en la comercialización y publicidad de productos financieros; y v) gestión diligente de reclamos y presentaciones.

Lo anterior se sustenta en los siguientes documentos:

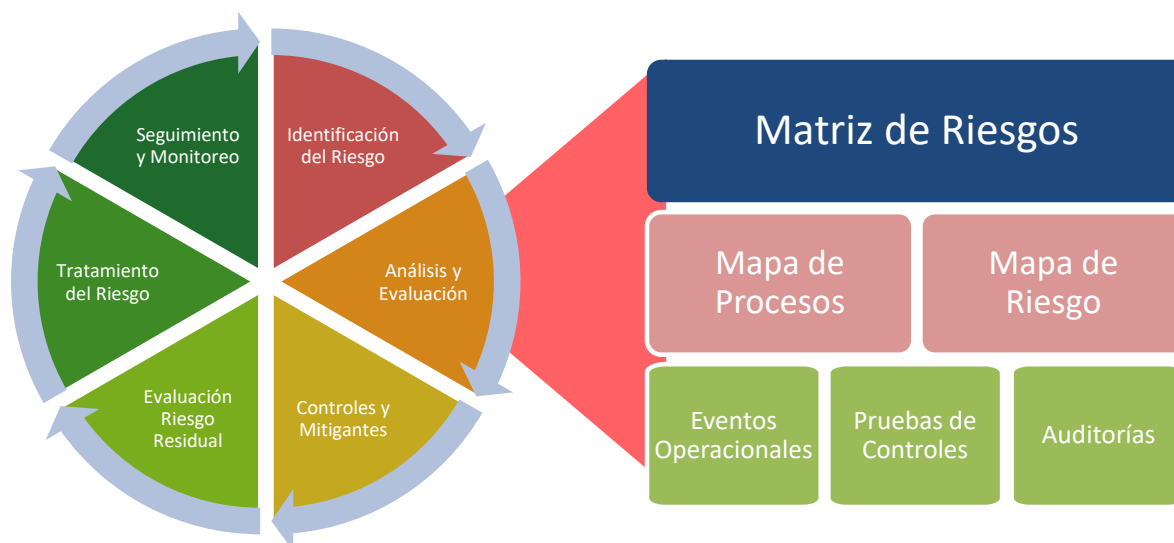
- **Política de Manejo de Información de Interés para el Mercado**
- **Política de Manejo de Información Privilegiada y Confidencial**
- **Política Anticorrupción y Conflicto de Interés**
- **Política y Procedimiento de Prevención de Delitos**
- **Política de Gestión de Reclamos**

8. Gobierno Corporativo

Se ha establecido un proceso formal de supervisión, el cual está estructurado por el Comité de Riesgo Operacional, el cual sesiona mensualmente, y que es presidido por un Director, y participa la alta administración de cada empresa. Esta instancia está estructurada en el Estatuto del Comité, donde se definen las funciones y se detalla su alcance. Organizacionalmente existe una línea directa de reporte al Directorio compuesta por, presentaciones trimestrales y reporte mensual del Comité al Directorio.

9. Política de Gestión de Riesgo Operacional

Se describen los lineamientos definidos para la gestión de riesgo operacional y las distintas etapas del ciclo de gestión vigente en la entidad, alineado con las buenas practicas del mercado brindadas por la ISO 31.000 de Gestión de Riesgo y se resume en el siguiente esquema.



9.1. Identificación del Riesgo Operacional

Es la etapa inicial del proceso cíclico de gestión de riesgo operacional, tiene como finalidad identificar los procesos de negocio generadores de riesgos, mapear o consumir un mapa de riesgo de la organización, identificación de los responsables de los procesos, subprocesos y actividades. Esta primera visión de los procesos permite tener un acercamiento inicial del alcance de las actividades, y contrastarlo con los objetivos estratégicos de la organización.

Junto a lo anterior, se determina cual o cuales normativas son aplicables a los procesos, sus exigencias y el cumplimiento de éstas. Finalmente, este levantamiento de información nutre inicialmente la matriz de riesgos.

Todo lo anterior se realiza basado en una revisión inicial de la documentación del proceso a evaluar, normativa vigente aplicable al proceso y por entrevistas con los responsables del proceso.

9.2. Análisis y Evaluación de Riesgo

Para analizar los riesgos identificados se utilizan escalas de evaluación, las cuales están graduadas en 5 niveles (Crítico, Alto, Moderado, Medio y Bajo), para clasificar un impacto y una probabilidad. Estas variables permiten obtener el resultado inicial del riesgo inherente de los procesos evaluados. Para esta evaluación se sugiere contar con información histórica de eventos operacionales ocurrido en los últimos años, volúmenes de operaciones, personas involucradas y otra estadística anexa que ayude a determinar la probabilidad y el impacto expuesto. El riesgo inherente es la exposición sin contar con la aplicación de controles o medidas mitigantes.

La documentación de este análisis y evaluación queda registrada en la matriz de riesgo, la cual es propuesta por el área de Riesgo Operacional y validada con el responsable del proceso.

9.3. Identificación de Controles y Mitigantes

El siguiente paso en el ciclo de gestión de riesgo es identificar los controles que tiene asociado el proceso evaluado para bajar la exposición al riesgo en términos de ocurrencia (probabilidad) o mitigantes al potencial impacto. Levantado los controles se procede a evaluar su eficacia frente al riesgo inherente, para esto se utilizan las siguientes variables:

- Evidencia del control
- Documentación
- Nivel de segregación
- Tipo de control
- Grado de automatización

El resultado de la determinación de las variables anteriores es el nivel de eficacia del control, el cual se documenta en la matriz de riesgo del proceso.

9.4. Evaluación del Riesgo Residual

El riesgo residual es el resultado de contrastar el riesgo inherente y el nivel de eficacia de los controles asociados a este riesgo, lo cual determina la parte del riesgo inherente que puede, eventualmente, materializarse en un evento implicando los potenciales impactos relacionados al riesgo. Los resultados se miden con la misma escala definida para el riesgo inherente. Este resultado queda documentado en la matriz de riesgo del proceso.

9.5. Apetito de Riesgo, Tolerancia y Tratamiento

El apetito de riesgo se define como “el total de riesgo que las entidades están dispuestas a aceptar para el cumplimiento de sus objetivos”¹

Este parámetro permite marcar una diferencia en el tratamiento de los riesgos y su priorización. En el marco de la presente política, el apetito de riesgo objetivo será un nivel de riesgo “Moderado”. Por lo tanto, para aquellos riesgos que resultan superior al apetito de riesgo definido, se debe tomar las medidas frente al diseño e implementación de controles que disminuyan la exposición al riesgo.

Respecto a la tolerancia al riesgo, se entiende como los niveles de variación que la entidad está dispuesta a aceptar en torno a objetivos específicos. Para esto se establece el lineamiento general siguiente:

- **Riesgos Bajos y Medios:** El tratamiento de estos riesgos es aceptar este nivel.
- **Riesgos Moderado:** Es el nivel que marca el apetito de riesgo objetivo. Por lo general se aceptará el riesgo, y puede requerir la definición de Indicadores Clave de Riesgo (KRI) para un monitoreo más frecuente.
- **Riesgos Altos y Críticos:** Requieren de una definición de plan de acción por parte del responsable del proceso y/o dueño del riesgo, por lo cual, junto al área de Riesgo Operacional deben formalizar las acciones para disminuir la exposición a estos niveles de riesgo. Se privilegiará la implementación de planes de acción que deriven en controles que disminuyan la frecuencia de ocurrencia de los riesgos. En casos donde no sea posible la implementación de controles, deben definirse e implementarse mitigantes que aminoren el impacto de la materialización de estos riesgos.

Para la gestión de riesgo asociados a la NCG N°510 de la CMF, se definen los siguientes apetitos de riesgos y tratamientos:

Riesgo	Bajo	Medio	Moderado	Alto	Crítico
Continuidad de Negocio	Se acepta	Se acepta	Decisión de tratar, transferir o aceptar a Directorio	Decisión de tratar, transferir o aceptar a Directorio	Tratar Transferir
Seguridad de la Información	Se acepta	Se acepta	Decisión de tratar, transferir o aceptar a Directorio	Decisión de tratar, transferir o aceptar a Directorio	Tratar Transferir
Ciberseguridad	Se acepta	Se acepta	Decisión de tratar, transferir o aceptar a Directorio	Decisión de tratar, transferir o aceptar a Directorio	Tratar Transferir
Externalización de Servicios	Se acepta	Se acepta	Se acepta	Tratar Transferir	Tratar Transferir

¹ Definición según COSO

9.6. Actividades de Seguimiento y Monitoreo

Las actividades asociadas al seguimiento y monitoreo contemplan todos los aspectos del proceso de gestión de riesgo operacional, con la finalidad de velar por el cumplimiento de los plazos e hitos comprometidos, diseño de los controles a implementar, proceso de implementación y estabilización de controles y/o mitigadores, y en general, todo plan de acción definido y comprometido para mejorar los procesos se lleve a cabo materializando el tratamiento de los riesgos asociados.

Por otro lado, se consideran los Indicadores Clave de Riesgo (KRI) para monitorear con una frecuencia mayor ciertos riesgos que, por su nivel de riesgo residual no requiera un plan de acción (riesgo moderado o menor), o que, siendo un riesgo que tratar, junto con el plan de acción sea necesario establecer un KRI para monitorear aspectos relevantes del proceso. Cada KRI debe contar con una Ficha de KRI, la cual documenta:

- Proceso asociado
- Riesgos
- Definición del KRI
- Umbrales de riesgo
- Descripción del KRI
- Responsables de entrega de información
- Responsables de planes de acción

10. Matriz de Riesgo

Es la herramienta fundamental para la gestión de riesgo de la entidad, dado que reúne los procesos, riesgos, controles, evaluaciones y planes de acción asociados a cada período de actualización. Permite identificar cuáles son los riesgos a los cuales la entidad se encuentra más expuesta y priorizar la toma de decisión para su tratamiento. Ésta matriz debe actualizarse a lo menos anualmente y contener la siguiente información:

- Identificación del proceso/ciclo de negocio
- Responsables del proceso
- Descripción y evaluación del riesgo inherente
- Controles asociados y su descripción
- Clasificación de la efectividad de los controles
- Evaluación del riesgo residual
- Tratamiento del riesgo residual

La matriz de riesgo da paso al mapa de riesgo de la entidad, el cual es la herramienta visual para identificar las exposiciones, niveles y cantidad de riesgos por niveles. Aquellos riesgos que se identifiquen en los cuadrantes alto o críticos deberán revisarse al menos semestralmente.

11. Eventos de Riesgo Operacional y Base de Pérdidas

Se define un evento de riesgo operacional como cualquier error, omisión o ineficiencias que afecte al proceso de negocio y no contribuya al objetivo de la entidad, lo cual genera impactos que van desde lo normativo a la pérdida económica. Es la materialización del riesgo operacional y su causa puede radicar en el proceso, el personal, los sistemas informáticos internos o servicios de proveedor o por causas externas a la entidad (ejemplo, fraude externo, robos, desastres naturales, ciberataques).

La gestión sobre estos eventos de riesgo operacional tiene como objetivo determinar la causa raíz y en base a esta información, identificar las acciones correctivas y las mejoras necesarias para bajar la exposición a estos fallos en los procesos. Estos eventos son presentados en el Comité de Riesgo Operacional.

Todo evento de riesgo reportado se registra en la Base de Eventos Operacionales (o Base de Pérdidas Operacionales), la cual reúne la información del evento, su clasificación, si tuvo o no pérdidas económicas asociadas directamente, junto al monto y si tuvo o no recuperaciones económicas y el monto.

La identificación de estos eventos de riesgo operacional puede concretarse por la comunicación de estos por parte de las áreas de negocio, según lo definido en el **“Procedimiento de Comunicación de Eventos Operacionales”** o, por medio de análisis independientes realizados por el área de Riesgo Operacional.

12. Testeo de Controles

Dentro de las actividades independiente definidas para el área de Riesgo Operacional se encuentran los Testeo o Pruebas de Controles, los cuales tiene por objetivo comprobar por medio de un análisis específico y dedicado la eficacia de los controles. Permite realizar un análisis de riesgo focalizado en partes del proceso, planteando las hipótesis, identificando métricas y parámetros a revisar, finalizando con una conclusión y, eventualmente, la definición de planes de acción para dar tratamiento a los riesgos y exposiciones comprobadas.

Estos testeos son propuestos en el Plan de Gestión de Riesgo Operacional y su resultado es expuesto en el Comité de Riesgo Operacional.

13. Plan de Gestión de Riesgo Operacional

El plan de gestión de riesgo operacional es una herramienta de planificación del trabajo para el año, en el cual se reúnen todas las actividades relevantes que deben ser presentadas y ser aprobada por el Comité de Riesgo Operacional y luego por el Directorio, entre los meses de febrero y marzo de cada periodo. Luego, el plan es revisado en cada sesión del Comité de Riesgo Operacional, marcando los avances e informando los incidentes que puedan afectar la ejecución de las actividades.

Por último, cada 6 meses, debe presentarse el plan a Directorio, o en menor tiempo, si es que hay cambios relevantes en la planificación de las actividades, las cuales requieren la aprobación de esta instancia.

14. Capacitación

Como parte del proceso de capacitación continua para el personal de la entidad y con el objetivo de conocer y gestionar con mayor eficacia los riesgos que se presentan en el desarrollo de las actividades, se establece un curso e-learning anual de Gestión de Riesgo y Control Interno, el cual es de carácter obligatorio, es realizado por todo el personal de la entidad, incluyendo a los miembros del Directorio.

15. Roles y Responsabilidades

A continuación, se definen los principales roles y responsabilidades asociados a la aplicación de la esta política.

15.1. Directorio

- Establecer la misión, visión y objetivos estratégicos de la entidad.
- Aprobar los niveles de apetito de riesgo.
- Revisar y aprobar las políticas de la entidad, previa aprobación del Comité de Riesgo Operacional.
- Establecer los procedimientos para la confirmación y funcionamiento de los comités de la entidad.
- Aprobar el plan del área de Riesgo Operacional.
- Evaluar periódicamente la suficiencia de recursos del área de Riesgo Operacional
- Conocer y comprender los riesgos inherentes de la entidad.
- Aprobar los sistemas y metodologías de medición y control de los distintos tipos de riesgos que enfrenta la entidad.
- Aprobar el plan de Auditoría Interna.

15.2. Comité de Riesgo Operacional

- Revisar y aprobar las políticas y manuales de procedimiento de la entidad.
- Informar al Directorio los resultados obtenidos de la gestión de riesgo de las áreas.
- Monitorear el estado de avance de las acciones comprometidas para resolver exposiciones al riesgo, y realizar seguimiento a la implementación de estas.
- Presentar y aprobar el plan de gestión de riesgo operacional
- Monitorear los resultados de los indicadores clave de riesgo (KRI).
- Informar al Directorio sobre situaciones de riesgo relevantes.
- Resolver discrepancias en el tratamiento del riesgo entre responsable del proceso y área de Riesgo Operacional.

15.3. Gerente General

- Revisar y aprobar, en primera instancia, las políticas y manuales de procedimiento de la entidad.
- Impulsar y supervisar la cultura de riesgo, valores y gobierno corporativo.
- Comunicar la estrategia y objetivos de la entidad, para alinear con los objetivos de la gestión de riesgo operacional.
- Monitorear el seguimiento permanente al cumplimiento de los límites de exposición al riesgo y medidas correctivas.

15.4. Área de Riesgo Operacional

- Responsable de aplicar la política de gestión de riesgo operacional en la entidad y mantener actualizada.
- Responsable de aplicar la metodología de gestión de riesgo operacional en la entidad.
- Mantener actualizado el manual de gestión de riesgo operacional.
- Mantener el seguimiento de las políticas y procedimientos de la entidad, controlando su vigencia, proponiendo mejoras y responsable del procedimiento de actualización.
- Efectuar el seguimiento permanente al cumplimiento de los límites de exposición al riesgo y de las medidas correctivas que se hubieren definidos para las deficiencias identificadas.
- Responsable de emitir informe trimestral al Directorio y al Gerente General para documentar las instancias de incumplimiento de límites, controles y acciones adoptadas ante tales circunstancias.
- Proponer cambios en las políticas y en los procedimientos de gestión de riesgos en función de las deficiencias encontradas en actividades de control.
- Monitorear la correcta corrección de las observaciones por falencias o deficiencias detectadas, tanto interna como externamente, que tengan implicancia en la gestión de riesgos de la entidad.

15.5. Área de Negocio

Las áreas de negocio se entienden por aquellas áreas que participan dentro de los procesos de negocios de la entidad. Y su rol y responsabilidad es:

- Gestionar el riesgo operacional de sus procesos.
- Reportar oportunamente eventos de riesgo operacional.
- Responsables de cumplir con el programa de capacitación.
- Aplicar los procedimientos definidos para gestión de riesgo.

15.6. Auditoría Interna

Constituye la tercera línea de defensa. Es una función independiente de las áreas de negocio y de la función de gestión de riesgos, con reporte directo al Directorio, encargada de proveer

aseguramiento sobre la efectividad del sistema de control interno y de la gestión de riesgos de la entidad. Sus principales responsabilidades son:

- Verificar el correcto funcionamiento del sistema de control interno y de gestión de riesgos, y su consistencia con los objetivos y políticas de la entidad, así como el cumplimiento de las disposiciones legales y normativas aplicables.
- Elaborar y ejecutar un plan anual de auditoría que asegure que las áreas, procesos, líneas de negocio o riesgos más relevantes, incluida la unidad de gestión de riesgos, sean auditados periódicamente.
- Evaluar la calidad y efectividad de las políticas, procedimientos, controles y mecanismos de control, incluyendo la efectividad del sistema de gestión de riesgos y la adecuada segregación de funciones.
- Identificar los incumplimientos de políticas y procedimientos detectados en las auditorías, sus causas, y verificar la adopción y el seguimiento de las medidas correctivas para evitar su reiteración.
- Calificar las observaciones detectadas y cada auditoría efectuada, conforme a categorías previamente definidas, y reportar oportunamente las deficiencias significativas al Directorio.
- Emitir al Directorio, a lo menos semestralmente, los informes que correspondan según el plan de revisión con las conclusiones, las medidas correctivas propuestas y sus plazos.
- Disponer de sistemas de información que permitan registrar sus actividades, programas de trabajo y resultados, y efectuar seguimiento a los compromisos adquiridos por las áreas auditadas en revisiones anteriores.
- Contar con personal con experiencia y conocimientos comprobables en los marcos de gestión de los riesgos que audita.

16. Excepciones

Se entiende por excepción toda situación en que, de manera justificada y temporal, se acepta mantener una exposición por sobre el apetito de riesgo definido, se supera un umbral de un Indicador Clave de Riesgo, o no resulta posible implementar un control comprometido dentro del plazo establecido. Toda excepción debe ser solicitada formalmente por el responsable del proceso o dueño del riesgo, con la justificación, el plazo de vigencia y las medidas mitigantes o el plan de acción asociados, y quedar debidamente documentada.

La autorización de las excepciones se efectúa conforme al nivel de riesgo involucrado: las asociadas a riesgos de nivel moderado son autorizadas por el área de Riesgo Operacional y ratificadas por el Comité de Riesgo Operacional, mientras que las asociadas a riesgos de nivel alto o crítico requieren la aprobación del Directorio.