METODOLOGÍA DE GESTIÓN DE RIESGO OPERACIONAL

TABLA DE CONTENIDO

I. INTRODUCCIÓN....4
II. OBJETIVOS DEL MANUAL....4
III. DOCUMENTOS REFERENCIADOS....4
IV. ALCANCE....4
V. DEFINICIONES....5
5.1. Alta Gerencia o Plana Ejecutiva....5
5.2. Cuasi-pérdidas....5
5.3. Dueño de Proceso/Líder del Proceso....5
5.4. Eventos de Pérdida de Riesgo Operacional....5
5.5. Clasificación de Eventos de Pérdida Derivados del Riesgo Operacional....5
5.6. Factores que Originan el Riesgo Operacional....6
5.7. Indicadores Claves de Riesgo Operacional....7
5.8. La Unidad de Riesgo Operacional (URO)....8
5.9. Metodología de Gestión del Riesgo Operacional....8
5.10. Pérdidas....8
5.11. Plan de Continuidad del Negocio (PCN)....8
5.12. Riesgo Operacional (RO)....8
5.13. Riesgo Legal (RL)....8
5.14. Riesgo Reputacional (RP)....8
5.15. Riesgo Estratégico (RE)....8
5.16. Riesgo Inherente (RI)....9
5.17. Riesgo Residual (RR)....9
5.18. Sistema de Gestión Riesgo Operacional ¨SGRO¨....9
5.19. Umbral....9
VI. SISTEMA DE GESTIÓN DEL RIESGO OPERACIONAL ¨SGRO¨....9
6.1. Objetivos específicos del Sistema ¨SGRO¨....9
6.2. Políticas Generales adoptadas....9
6.3. Políticas sobre Indicadores Claves de RO....10
6.4. Políticas de Subcontratación o Tercerización....10

6.5. Políticas y Planes de Continuidad de Negocio 11
6.6. Evaluación de Riesgos para la Incorporación y/o Modificación de Productos/Servicios 11
6.7. Evaluación del Sistema de Seguridad de la Información 11
VII. ESTRUCTURA ORGANIZACIONAL 12
VIII. RESPONSABILIDADES Y ROLES 13
8.1. Responsabilidades del Directorio 14
8.2. Responsabilidad de la Gerencia General 14
8.3. Responsabilidades de la Unidad de Gestión de Riesgo Operacional 15
8.4. Responsabilidades del Jefe de División Organización y Procesos 15
8.5. Responsabilidades de los Dueños de Procesos 16
8.6. Responsabilidades de los Gestores Riesgo Operacional (GRO) 16
8.7. Responsabilidad de Gerencia de Área de Auditoria Interna 16
8.8. Responsabilidad del Comité de Riesgo 16
IX. DEFINICIONES Y CRITERIOS DE RIESGOS 17
9.1. Apetito y Tolerancia al Riesgo 17
9.2. Umbrales Monto Máximo de Pérdidas Totales 17
9.3. Umbral para la registración y el seguimiento de eventos de Riesgo Operacional 17
9.4. Umbral para la registración y evaluación de las cuasi-pérdidas 17
X. PROCESO DE GESTIÓN DE RIESGO OPERACIONAL DEL BNF 17
10.1. Etapas del Proceso de Gestión del Riesgo Operacional 17
10.2. Valoración de Riesgos Inherentes 20
10.3. Matriz de Riesgos 20
10.4. Evaluación de los Controles 21
10.4.1 Efectividad 21
10.4.2 Diseño 21
10.5. Registro del Mapa de Riesgos 22
10.6. Matriz de Riesgo Residual 22
10.7. Tratamiento del Riesgo 23
10.8. Monitoreo del Perfil de Riesgo 23
10.9. Registro de Eventos de Riesgo 24
XI. INFORMES GERENCIALES 24
XII. DIVULGACIÓN Y CAPACITACIÓN 24
XIII. AUDITORÍA INTERNA 25

XIV. REVISIÓN DEL MANUAL 25
ANEXO I.....26
a) Tabla de Impacto/ Probabilidad.....26
b) Definición de Umbrales.....28

I. INTRODUCCIÓN

En materia de Riesgo Operacional, desde la puesta en vigencia de la Resolución N° 4~~,~~ Acta 67~~,~~ de fecha 27 de diciembre del 2012, emitida por el Banco Central del Paraguay, que establece las reglas relativas a la Administración del Riesgo Operacional para que las entidades sometidas a su vigilancia y control adopten, establezcan, implementen y administren adecuadamente un Sistema de Gestión del Riesgo Operacional, el Banco Nacional de Fomento (BNF) ha ido implantando medidas para la identificación, análisis, evaluación, seguimiento, control y tratamiento de este tipo de riesgo.

Este tipo de gestión se ubica en el contexto de la cultura general, en las capacidades y habilidades de la entidad para convivir y colaborar con las estrategias generales. Significa que la Gestión del Riesgo Operacional debe planificarse con el involucramiento de las diferentes áreas de la entidad, y por ello la implementación de la administración de este tipo de riesgo debe estar incluida en un documento orientador que establezca las directrices que la institución adopta para tal implementación.

La entidad debe gestionar el riesgo operacional, como elemento fundamental de una administración preventiva que reduzca al mínimo la posibilidad de pérdidas, e incremente su eficiencia, para lo cual deberá implementar mecanismos, procesos y contar con recursos humanos calificados y experimentados, siguiendo los delineamientos de las normativas locales y las mejores prácticas en el mercado.

El presente documento establece los lineamientos generales, que deberá observar el **BNF**, para gestionar el riesgo operacional.

II. OBJETIVOS DEL MANUAL

Este Manual tiene el propósito de establecer los lineamientos y políticas a ser adoptados en la implementación de una Metodología de Gestión de Riesgo Operacional, cuyo objetivo es el de monitorear, medir y controlar los riesgos operacionales implícitos en los procesos del BNF.

III. DOCUMENTOS REFERENCIADOS

- Resolución SIB N° 4/2012 Reglamento para la Gestión del Riesgo Operacional.
- Circular SIB N° 65/2010 Reglamento que establece los estándares mínimos para un buen Gobierno Corporativo.

IV. ALCANCE

El presente Manual contiene los elementos de la Metodología de Gestión de Riesgo Operacional de la entidad, el cual inicia con la identificación y medición de los eventos de riesgo operacional en cada uno de los procesos que involucra a las operaciones, para luego establecer y monitorear los controles y el perfil de riesgo del banco.

La gestión del Riesgo Operacional es responsabilidad de todo el personal del BNF, incluyendo al Directorio, las Gerencias, las Divisiones, Secciones y a los funcionarios de la entidad.

Las responsabilidades se distribuyen de la siguiente manera:

- Definición de una *Estrategia adecuada para la Gestión del Riesgo Operacional*, es responsabilidad del Directorio.

- La *Gestión y Mantenimiento* del Sistema de Gestión de Riesgo Operacional es responsabilidad de la Gerencia de Área de Riesgos, apoyado por la Gerencia Departamental de Gestión de Riesgo Integral y la División Riesgos Operativos.
- La *Evaluación y el Tratamiento* del Riesgo Operacional está a cargo de los Dueños de Procesos, apoyados en los Gestores de Riesgos designados por los mismos.
- El *Monitoreo del Cumplimiento* de Políticas y Procedimientos de Riesgo Operacional corresponde a Auditoría Interna.

V. DEFINICIONES

Para los fines de este documento, se aplican los términos y definiciones contenidos en la Metodología de Gestión Integral de Riesgos, sobre Apetito de Riesgo, Control, Evento, Perfil de Riesgo y Umbral.

5.1. Alta Gerencia o Plana Ejecutiva

Son los responsables de ejecutar las disposiciones del Directorio, quienes toman decisión de alto nivel de acuerdo con las funciones asignadas y la estructura organizacional definida en cada entidad. El BNF define que la Alta Gerencia constituye la Gerencia General, las Gerencias de áreas y; junto con los Gerentes Departamentales formarán la Plana Ejecutiva.

5.2. Cuasi-pérdidas

Eventos que no llegaron a derivar en pérdidas financieras, es decir no tienen impacto económico porque se identifican antes de que el riesgo se materialice (ejemplo: error en un contrato que se detecta antes de que sea firmado, error en condiciones de una operación que se detecta antes de ser incluida en el sistema que la procesa)

5.3. Dueño de Proceso/Líder del Proceso

Es el responsable de la correcta ejecución de los procesos a su cargo y de administrar el mejoramiento continuo del mismo en coordinación con la División de Organización y Procesos y por recomendaciones hechas por la Gerencia de Área de Riesgos o la Gerencia de Área de Auditoria Interna.

5.4. Eventos de Pérdida de Riesgo Operacional

Son aquellos incidentes o hechos que puede derivar en pérdidas financieras por Riesgo Operacional a la entidad.

5.5. Clasificación de Eventos de Pérdida Derivados del Riesgo Operacional

5.5.1 Fraude Interno: Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiación de bienes indebidamente o incumplir regulaciones, leyes, por parte de al menos un funcionario del BNF, que tiene como fin obtener un beneficio ilícito.

5.5.2 Fraude Externo: Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir la legislación, por parte de un tercero, con el fin de obtener un beneficio ilícito.

5.5.3 Relaciones laborales y seguridad en el puesto de trabajo: Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamos por daños personales o sobre casos relacionados a discriminación.

5.5.4 Prácticas con clientes, productos y negocios: Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación frente a clientes concretos o de la naturaleza y diseño de un producto.

5.5.5 Daños a activos físicos: Pérdidas derivadas de daños o perjuicios a activos físicos de la Entidad, como consecuencia de desastres naturales, actos de terrorismo, vandalismo u otros acontecimientos.

5.5.6 Interrupción del negocio y fallos en los sistemas: Pérdidas derivadas de interrupciones en el negocio e incidentes por fallas tecnológicas, problemas en telecomunicaciones, interrupción de servicios públicos, entre otras.

5.5.7 Ejecución, gestión y cumplimiento del plazo de los procesos: Pérdidas derivadas de errores en la ejecución y administración de los procesos, así como en relaciones con contrapartes comerciales y proveedores.

La clasificación del Riesgo por clases y factores se despliega en el siguiente cuadro:

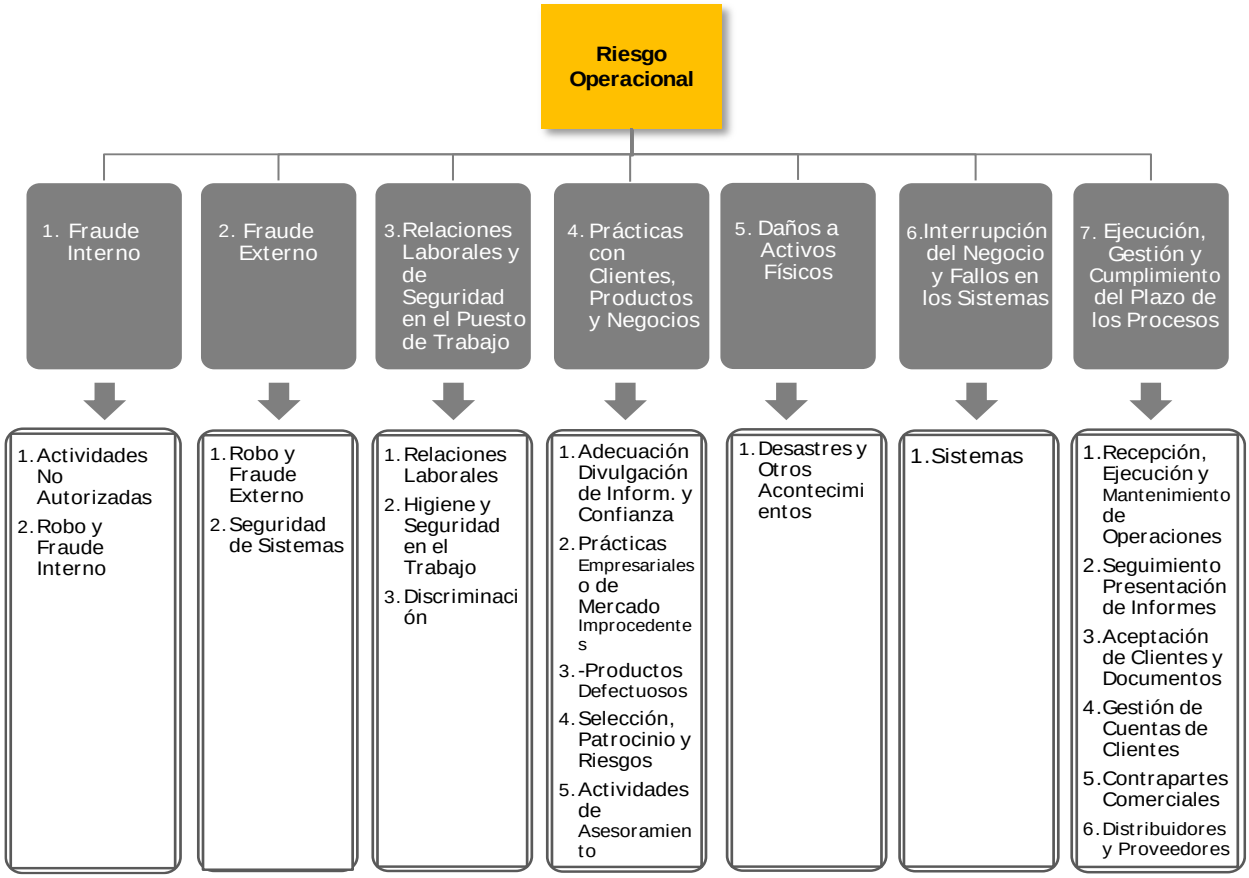

Figura 1: Clasificación del Riesgo por Clases y Factores de Riesgo

5.6. Factores que Originan el Riesgo Operacional

Se entiende por factores de riesgo, la causa primaria o el origen de un evento de riesgo. Los factores son: los procesos, personas, tecnología de la información y eventos externos. A su vez se clasifican en internos o externos, según se indica a continuación:

5.6.1 **Factores Internos:**

a) **Procesos Internos:** Es el conjunto de actividades que transforman los elementos de entrada en productos o servicios, ya sea para satisfacer las necesidades del cliente interno o externo.

La institución incorpora en su operativa la aplicación de delineamientos de la gestión por procesos basados en las mejores prácticas.

El Dueño de Proceso y/o Gestor de Riesgo Operacional debe gestionar los riesgos asociados a los procesos internos implementados para realizar sus operaciones y servicios. La ausencia de procedimientos, o la desactualización de acuerdo con la operativa actual, o procedimientos inadecuados, pueden tener como consecuencia el desarrollo deficiente de las operaciones, la evaluación incorrecta u omisión de los riesgos operativos, así como la suspensión de la operativa.

b) **Personas:** Son los individuos vinculados directa o indirectamente con la ejecución de los procesos de la institución.

La institución debe gestionar los riesgos asociados al personal, a través del establecimiento de programas de capacitación acorde a la posición o el cargo, manteniendo la cantidad adecuada de recursos en especial en los cargos que ejercen control, además de velar por una adecuada segregación de funciones. Las políticas y procedimientos establecidos para la incorporación, permanencia y desvinculación del personal de la institución se encuentran contempladas en las documentaciones de referencia, además de las exigencias regulatorias aplicadas a la Función Pública.

c) **Tecnología de la Información:** Es el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software y telecomunicaciones.

La institución deberá gestionar los riesgos asociados a la Tecnología de la Información basadas en las disposiciones contenidas en las ***Manual de Gobierno y Control de Tecnología de la Información del BNF;*** además de las exigencias regulatorias dictaminadas por la Superintendencia de Bancos (SIB).

5.6.2 **Factores Externos:**

Son eventos adversos asociados a la fuerza de la naturaleza u ocasionados por terceros, que escapan en cuanto a su causa y origen al control de la institución, tales como: fallas en los servicios públicos, epidemias y/o pandemias, ocurrencia de desastres naturales, atentados y otros actos delictivos. Para el efecto el BNF dispone de los planes de contingencia y de continuidad del negocio, de acuerdo con los delineamientos definidos en el Manual de Continuidad del Negocio.

5.7. Indicadores Claves de Riesgo Operacional

Constituyen alarmas tempranas indicadas en los sistemas, procesos, productos, personas y el ambiente externo, basadas en estadísticas y/o parámetros, tales como número de operaciones fallidas, rotación del personal, la frecuencia y/o gravedad de los errores, entre otros.

5.8. La Unidad de Riesgo Operacional (URO)

Se entiende por Unidad de Riesgo Operacional el área designada por la entidad, que debe gestionar y coordinar la puesta en marcha y mantenimiento de la Metodología de Gestión del Riesgo Operacional. El BNF designó a la Gerencia de Área de Riesgos y sus dependencias Gerencia Departamental de Gestión de Riesgo Integral y la División Riesgos Operativos como URO; de manera matricial también son parte de la Unidad de Riesgo Operacional los Gestores de Riesgo Operacional de las diferentes áreas del Banco.

5.9. Metodología de Gestión del Riesgo Operacional

Es el documento que contiene las políticas, objetivos, conceptos y definiciones, estructura organizacional de la URO, estrategias, y referencia a los procesos y procedimientos aplicables en el desarrollo, implementación y seguimiento de la Gestión de Riesgo Operacional.

5.10. Pérdidas

Cuantificación económica de la ocurrencia de un evento de Riesgo Operacional, así como los gastos derivados de su atención.

5.11. Plan de Continuidad del Negocio (PCN)

Es un conjunto de recursos y procedimientos que permiten mantener y recuperar en el menor tiempo y costo posible los procesos críticos de la Entidad ante una contingencia dada.

5.12. Riesgo Operacional (RO)

Es la posibilidad de sufrir pérdidas debido a la falta de adecuación o fallas de los procesos internos, personas, sistemas o eventos externos. Incluye el riesgo legal, pero excluye el riesgo estratégico y reputacional.

5.13. Riesgo Legal (RL)

Es la posibilidad de que se presenten pérdidas o contingencias negativas como consecuencia de fallas en la ejecución de los contratos, acuerdos o transacciones, que pueden afectar el funcionamiento de la institución, derivadas de error, negligencia o imprudencia en la concertación, instrumentación, formalización o ejecución de estos; así como de incumplimientos de leyes o normativas aplicables.

5.14. Riesgo Reputacional (RP)

El riesgo de reputación es la posibilidad de pérdida en que puede incurrir la entidad por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto del BNF y sus prácticas de negocios, por parte del público (clientes actuales y potenciales, contrapartes, empleados, inversores y reguladores) o de otros sectores (medios, sindicatos, sociedad en general) que cause pérdida de clientes o reducción de la rentabilidad

5.15. Riesgo Estratégico (RE)

Los riesgos estratégicos son aquellos riesgos que pueden afectar a la capacidad del BNF para alcanzar sus objetivos y metas generales.

5.16. Riesgo Inherente (RI)

Nivel de riesgo propio de la actividad y/o del proceso, sin tener en cuenta el efecto de los controles.

5.17. Riesgo Residual (RR)

Nivel resultante del riesgo después de aplicar los controles.

5.18. Sistema de Gestión Riesgo Operacional ¨SGRO¨

El Sistema de Gestión del Riesgo Operacional ¨SGRO¨ es el conjunto de elementos tales como la Metodología, las políticas, procedimientos, documentación, estructura organizacional, registro de eventos de Riesgo Operacional, órganos de control, plataforma tecnológica, divulgación de la información y capacitación, mediante los cuales la institución identifica, mide, controla y monitorea el Riesgo Operacional.

5.19. Umbral

Consiste en la definición de un valor que permite conocer a partir de qué momento se necesita tomar una acción o simplemente no hacer nada, en caso de que esté por debajo de dicho valor. Los umbrales responderán al nivel de apetito de riesgo que desea tener la institución para poder aceptar o no determinados niveles esperados de eventos de riesgo operacional.

VI. SISTEMA DE GESTIÓN DEL RIESGO OPERACIONAL ¨SGRO¨

6.1. Objetivos específicos del Sistema ¨SGRO¨

a. Identificar en los procesos evaluados, los eventos de riesgo, establecer un perfil de riesgo y asegurar que los controles se ajusten en la medida que se desarrolle la cultura de prevención del Riesgo Operacional.

b. Establecer las metodologías de identificación, registro y valoración del Riesgo Operacional.

c. Establecer los métodos para registrar los eventos de Riesgo Operacional, así como las pérdidas que pudieren presentarse.

d. Divulgar el sistema y capacitar a los funcionarios en cada una de las etapas del proceso de evaluación de Riesgo Operacional.

e. Asegurar que los eventos de riesgos identificados sean registrados en la Base de Datos de Eventos y Pérdidas.

f. Velar porque el riesgo sea controlado y mitigado permanentemente.

g. Asegurar la actualización y verificación del sistema de acuerdo con las mejoras metodológicas y/o nuevos productos o servicios que se llegaren a prestar a los clientes, así como la permanente divulgación y capacitación a los funcionarios.

6.2. Políticas Generales adoptadas

- El BNF definió e implantó un sistema que permite identificar, registrar, medir, controlar y monitorear los Riesgos Operacionales. Para el efecto asigna a una unidad organizacional la administración y mantenimiento del sistema que verifica el cumplimiento de las normas internas y externas que se establecen en esta materia.

- La administración del Sistema de Gestión de Riesgo Operacional está a cargo de la División Riesgos Operativos que es una unidad especializada, con la adecuada independencia de otros riesgos para desarrollar sus funciones.
- El BNF impulsa a nivel institucional una cultura de prevención del Riesgo Operacional acorde con otras políticas y otros sistemas como los de Riesgo Crediticio, Financiero y de Mercado.
- El Sistema de Gestión del Riesgo Operacional debe ser dinámico de tal forma que se asegure la identificación de cambios en los controles y perfiles de riesgo, permita la actualización del nivel de riesgo y facilite a su vez la prevención y resolución de conflictos de interés en la recolección de la información durante sus diferentes etapas de implementación, así como en el registro de eventos y en el mantenimiento del sistema.
- Las funciones y competencias de cada uno de los funcionarios, así como la estructura organizacional, deben mantenerse adecuadas a los propósitos y requerimientos del sistema y deben ser incluidos en los respectivos manuales de Descripción de Funciones.
- Toda excepción a lo establecido en el presente manual debe ser autorizada por el Directorio, a instancia de la Gerencia General. El Directorio podrá delegar a la Gerencia General determinadas facultades en uso de sus atribuciones.

6.3. Políticas sobre Indicadores Claves de RO

Otra herramienta que el BNF podrá utilizar para identificar, evaluar y/o monitorear sus riesgos operacionales, es la utilización de Indicadores Claves de Riesgo Operacional (Key Risk Indicators o KRI), que deberán ser utilizados por los Dueños de Proceso y revisados con la periodicidad que se establezca, para monitorear sobre cambios que podrían indicar un mayor riesgo.

Al definir los Indicadores Claves de Riesgos de RO, se deberá asignar a los mismos, unos límites, un proceso de seguimiento eficaz, responsables del monitoreo, de manera que puedan constituirse en alarmas para las áreas dueñas de procesos, quienes evaluarán su posición ante el riesgo, y al Comité de Riesgos que acompañará a las áreas en la toma de decisiones (mitigar, transferir o asumir riesgos operacionales).

6.4. Políticas de Subcontratación o Tercerización

Con el fin de administrar los riesgos relevantes vinculados a la Tercerización de Servicios ya sea de las actividades y/o procesos esenciales para la institución (procesos críticos) y con el entendimiento de que este tipo de servicios no exime al BNF ni al Directorio de la responsabilidad primaria que conlleva a la ejecución de las mismas, las Gerencias de áreas responsables de solicitar los servicios deberán efectuar las evaluaciones respectivas al proveedor (como parte del proceso de Contrataciones) y supervisar esta línea de procesos ejecutados, manteniendo una fluida comunicación con la Subgerencia Departamental Operativa de Contrataciones y la División Riesgos Operativos.

A fin de resguardar el control sobre las funciones/procesos/servicios que sean objeto de Tercerización, se deberá contemplar en los términos de referencia (antes de la contratación) principal y explícitamente lo siguiente:

- Los límites de la responsabilidad de terceros frente a la institución.

- El requerimiento de la capacidad financiera para casos de indemnización en concepto de errores, negligencia o cualquier otro fallo operativo.
- Verificar y requerir a terceros proteger la información confidencial de la propia entidad como de sus clientes de divulgaciones no autorizadas.
- El requerimiento de contar con planes de continuidad implementados.

El proceso de contratación del Proveedor se efectuará conforme al marco normativo de Contrataciones Públicas y las políticas internas establecidas en el **Manual de Contrataciones del BNF.**

6.5. Políticas y Planes de Continuidad de Negocio

Con el fin de administrar los riesgos operacionales vinculados a los eventos externos ante la pérdida derivada de la ocurrencia de eventos ajenos a su control tales como: fallas en los servicios públicos, ocurrencia de desastres naturales, atentados y otros hechos delictivos, los cuales pudieran alterar el desarrollo normal de sus actividades, el BNF dispone de ***Políticas y Planes de Continuidad de Negocio***, administrados por la Gerencia de Área de Riesgos.

6.6. Evaluación de Riesgos para la Incorporación y/o Modificación de Productos/Servicios

En forma previa al lanzamiento o presentación de un nuevo producto/servicio (inicio de actividades, puesta en marcha de aspectos operativos o informáticos relacionados a dicho producto/servicio), deberá comprobarse una adecuada Gestión del Riesgo Operacional a efectos de asegurar que todos los riesgos involucrados cuentan con adecuados controles que los mitiguen.

Los criterios para la evaluación del riesgo integral y operacional en la Incorporación y/o Modificación de Nuevos Productos/Servicios se encuentran definidos en el Manual de Procedimientos de Riesgo Operacional, en la sección denominada:

- Procedimiento de “Evaluación de Riesgos en la Incorporación y/o Modificación de Productos/Servicios”.

6.7. Evaluación del Sistema de Seguridad de la Información

Con el fin de tratar los riesgos asociados a los procesos de Seguridad de la Información (SI) y los activos de información de la institución, la Gerencia Departamental de Administración de Seguridad de TIC del BNF estará a cargo de realizar las evaluaciones de riesgos operacionales de los procesos de SI, y definir y gestionar el Plan de Tratamiento de Riesgos de Seguridad de la Información, bajo los delineamientos y estándares definidos por el Directorio, para un mayor alcance de la gestión del riesgo en la seguridad de la Información.

La División Riesgos Operativos estará en constante comunicación con el área de Seguridad de la Información a fin de reforzar la evaluación y el tratamiento de los riesgos operacionales.

VII. ESTRUCTURA ORGANIZACIONAL

Para el cumplimiento de los objetivos de implementar el Sistema de Gestión de Riesgo Operacional, el banco cuenta con una Estructura Organizacional adecuada para esos fines, la cual se encuentra organizada de la siguiente manera:

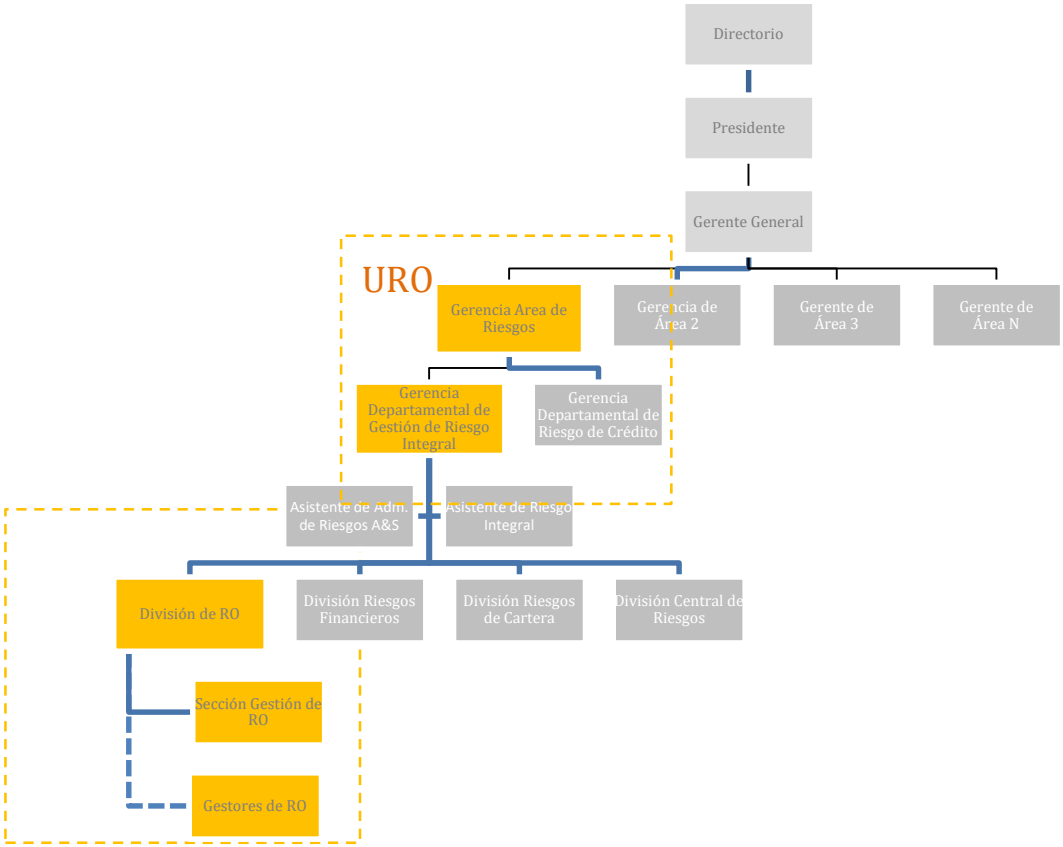

Figura 2: Ubicación de la Unidad de RO en la Estructura Organizacional

La Unidad de Riesgo Operacional deberá contar con el personal y la infraestructura necesaria para cumplir con los objetivos del Sistema de Gestión del Riesgo Operacional; en consecuencia, es el área responsable de administrar y mantener el sistema y de comunicar a la Alta Dirección las novedades que se presenten al respecto.

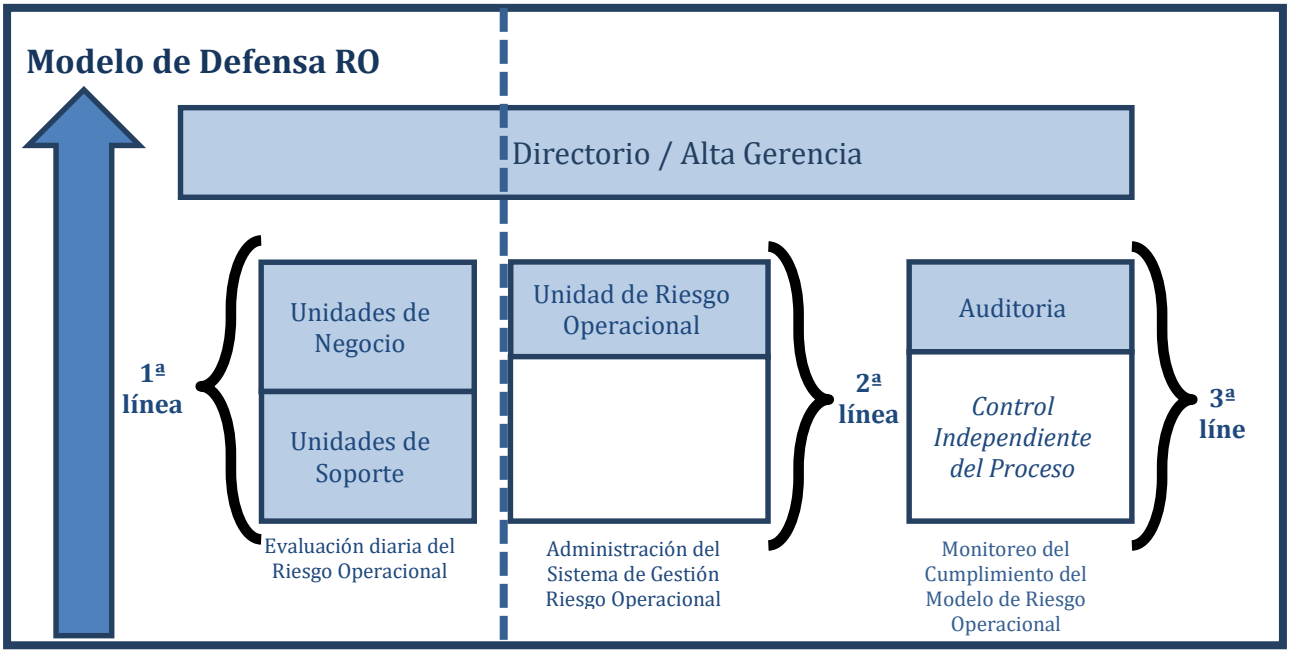

Figura 3: Modelo de defensa de Riesgo Operacional

La figura adjunta señala la distribución de responsabilidades; considerando el modelo adoptado por el Banco en la gestión integral del riesgo, existen tres líneas de defensa para la institución con el fin de permitir una eficiente y eficaz gestión de sus riesgos operacionales.

Este modelo es la forma en que se distribuyen las responsabilidades de administración de Riesgo en la institución.

Las Gerencias/Responsables de Áreas del BNF, junto con las Gerencias Departamentales y las Divisiones respectivas tienen la principal responsabilidad frente a la evaluación y administración de sus riesgos, actividad que deben realizar en el día a día. Esta constituye la primera línea de defensa.

La Unidad de Riesgo Operacional tiene la responsabilidad de gestionar el Modelo de Gestión de Riesgo Operacional, así como las Políticas de Riesgo Operacional. Esta constituye la segunda línea de defensa.

La Gerencia de Área de Auditoria Interna tiene la responsabilidad de proveer una visión independiente acerca del Sistema de Gestión de Riesgo Operacional. Esta constituye la tercera línea de defensa.

VIII. RESPONSABILIDADES Y ROLES

Sin perjuicio de lo definido en el Manual de Organización y Funciones del BNF, el Código de Buen Gobierno del BNF y en las Leyes 281 y 751/ 1961 de creación del BNF y/o en las reglamentaciones locales

para la Función Pública, se establecen las siguientes responsabilidades para cada función definida en el Modelo de Riesgo Operacional:

8.1. Responsabilidades del Directorio

El Directorio es responsable que la institución cuente con una estrategia adecuada para la Gestión del Riesgo Operacional, incluyendo:

a. Aprobar la implementación de un marco para la gestión del Riesgo Operacional como un riesgo diferente, teniendo en cuenta las dimensiones del BNF y la complejidad de sus operaciones, con una periodicidad mínima de revisión o cada vez que se produzcan hechos o situaciones de relevancia vinculadas con este riesgo.

b. Aprobar la Metodología de Gestión del Riesgo Operacional.

c. Suministrar pautas y directrices claras a la Gerencia General y aprobar las políticas correspondientes desarrolladas por la Unidad de Riesgo Operacional.

d. Tomar conocimiento de los procedimientos desarrollados a efectos de gestionar el Riesgo Operacional y su grado de cumplimiento, para ello, deberá recibir información con una periodicidad adecuada, la información suficiente que permita analizar el perfil de Riesgo Operacional de la institución y verificar sus implicancias estratégicas y sustanciales para su actividad.

e. Asegurar que el proceso esté sujeto a un examen de Auditoria Interna eficaz e integral.

f. Asignar los recursos necesarios para la adecuada gestión del Riesgo Operacional, a fin de contar con la infraestructura, metodología, capacitación y personal apropiados.

g. Aprobar políticas de difusión en el marco de la Gestión de Riesgo Operacional, de capacitación, dirigida a todas las áreas y funcionarios de la institución.

h. Aprobar políticas para la gestión de los riesgos operacionales derivados de actividades de los servicios prestados por los proveedores.

i. Garantizar una estructura capaz de implementar y mantener el marco de administración del Riesgo Operacional de la institución, que deberá contar con personal técnico capacitado en este riesgo.

j. Verificar que la Unidad de Riesgo Operacional no desarrolle otras tareas en áreas que puedan generar conflictos de intereses con su función.

8.2. Responsabilidad de la Gerencia General

a. Asegurar que el BNF cuente con estructuras y procesos apropiados para una gobernanza efectiva relacionada a los riesgos operacionales.

b. Impulsar las acciones presentadas por la Gerencia de área de Riesgos sobre los planes y programas que tienen por objetivo fortalecer la cultura de riesgos operacional institucional.

c. Mantener comunicación constante entre las Gerencias a su cargo con el fin de asegurar el cumplimiento de las políticas relacionadas al riesgo operacional.

d. Dar seguimiento para la puesta en práctica y funcionamiento del marco de gestión aprobado por el Directorio del BNF, de manera que todos los niveles del personal entiendan sus responsabilidades respecto a la administración de este riesgo.

e. Establecer líneas claras de autoridad, responsabilidad y comunicación con las distintas áreas de la institución.

f. Evaluar y aprobar la estructura que la Gerencia de Área de Riesgos presente, que sea capaz de implementar el marco de administración del Riesgo Operacional de la institución, que deberá contar con personal técnico capacitado en este riesgo.

g. Asegurar que el responsable por la administración del riesgo operacional trabaje en coordinación con los responsables de la administración de los demás riesgos.

h. Informar periódicamente al Directorio, los principales aspectos relacionados con la Gestión de Riesgo Operacional.

8.3. Responsabilidades de la Unidad de Gestión de Riesgo Operacional

a. Diseñar y Desarrollar las políticas, procesos y procedimientos para la administración del riesgo operacional.

b. Participar en el diseño y desarrollar la metodología para la Gestión del Riesgo Operacional, que deberá ser implementada en forma consistente en toda la Institución.

c. Asesorar a las áreas en la evaluación del riesgo en forma previa al lanzamiento de nuevos productos/servicios y ante cambios importantes en el aspecto operativo e informático.

d. Identificar las necesidades de capacitación y difusión para una adecuada gestión del Riesgo Operacional.

e. Informar al Comité de Riesgos, la Gerencia General y el Directorio la detección de posibles deficiencias que se produzcan en la aplicación de políticas, procesos y procedimientos de gestión de Riesgo Operacional y proponer las correcciones a las mismas, con la periodicidad establecida por la Institución

f. Asesorar a los Dueños del Proceso y Gestores de Riesgos Operacional, para el cumplimiento de los procedimientos de gestión de Riesgo Operacional.

g. Mantener una estrecha comunicación con las diferentes áreas que podrían detectar riesgos como áreas de control interno, de contratación de servicios externos, subcontrataciones, etc.

En el Manual de Organización y Funciones del BNF se encuentran definidas estas funciones de una manera más detallada.

8.4. Responsabilidades del Jefe de División Organización y Procesos

a. Proveer a la División Riesgos Operativos la información de cuáles son los procesos críticos de la institución con el fin de establecer el plan anual de identificación y evaluación de los riesgos operativos en forma preventiva para trabajar con las diferentes áreas.

b. Asesorar en la identificación de procesos, subprocesos, y actividades para nuevos productos, servicios o canales o por modificaciones de procesos y productos existentes a fin de que se puedan identificar y evaluar los riesgos inherentes a los mismos.

8.5. Responsabilidades de los Dueños de Procesos

a. Reconocer e identificar los procesos críticos en función a su importancia estratégica y potencial de mejora.

b. Participar en las sesiones de evaluación del Riesgo Operacional, cuando sea necesario.

c. Aprobar la evaluación de riesgos realizada por el Gestor de Riesgo Operacional, sobre los procesos.

d. Implementar, aplicar, mantener y actualizar el Sistema de Control Interno de su área, cuyas acciones preventivas y correctivas, permitirán la mitigación del Riesgo Operacional.

e. Elaborar, establecer y mantener actualizadas las políticas y procedimientos de los cuales son responsables.

f. Definir e implementar los planes de mitigación de eventos de pérdidas por Riesgo Operacional.

g. Reportar los eventos de pérdidas y cuasi perdidas registrados en su área, al momento de la toma de conocimiento de su ocurrencia, vía Gestor de Riesgo Operacional.

h. Mantener una estrecha comunicación con su área, así como con la Unidad de Riesgo Operacional con relación al Riesgo Operacional que contribuya a una mejora continua.

i. Informar y difundir reportes de acuerdo con la metodología emitida por la División Riesgos Operativos y fomentar la cultura de Riesgo Operacional.

8.6. Responsabilidades de los Gestores Riesgo Operacional (GRO)

a. Identificar y evaluar los riesgos operacionales detectados, determinando las causas y efectos derivados a los riesgos identificados.

b. Determinar cada vez que sea identificado un riesgo, la frecuencia e impacto económico para aquellos riesgos cuantificables por pérdidas directas.

c. Identificar y realizar la evaluación de los controles del proceso evaluado.

d. Proporcionar información relacionada con el seguimiento de las acciones referentes a los planes de mitigación.

e. Reportar y registrar los eventos de pérdidas y cuasi perdidas identificados en su área, a través del Dueño del Proceso, al momento de la toma de conocimiento de su ocurrencia.

f. Mantener una estrecha comunicación con su área, así como con la Unidad de Riesgo Operacional con relación al Riesgo Operacional que contribuya a una mejora continua.

8.7. Responsabilidad de Gerencia de Área de Auditoria Interna

a. Proveer una visión independiente acerca del Sistema de Gestión de Riesgo Operacional.

8.8. Responsabilidad del Comité de Riesgo

Las funciones y responsabilidades del Comité encargado de tratar los temas de la gestión de riesgo operacional se encuentran detalladas en el documento ***"Res. N° 15 Acta 44 14-06-18 BNF Manual de Funciones del Comité de Riesgos".***

IX. DEFINICIONES Y CRITERIOS DE RIESGOS

9.1. Apetito y Tolerancia al Riesgo

Tomar riesgos es un componente necesario de cualquier actividad empresarial. En el BNF nuestro objetivo es asegurar que los riesgos tomados sean identificados, apropiadamente evaluados, controlados y mitigados (cuando sea apropiado). El Apetito y Tolerancia al Riesgo Operacional está alineado al Riesgo Integral del Banco y se encuentra detallado en la ***Metodología de Gestión Integral de Riesgos - Declaración del Apetito por el Riesgo.***

9.2. Umbrales Monto Máximo de Pérdidas Totales

Es el monto máximo de pérdidas totales (sumatoria de eventos) que tolerará la institución por riesgo operativo, en el periodo de un año fiscal. Los montos se encuentran indicados en el Anexo I.

9.3. Umbral para la registración y el seguimiento de eventos de Riesgo Operacional

- **El Umbral para la registración**: es el importe definido a partir del cual se realizará el registro del evento de pérdida por riesgo operativo en la base de datos.
- **El Umbral para Seguimiento de eventos de pérdida de Riesgo Operacional**: es el importe desde el cual se realiza el seguimiento de eventos de pérdida. Los montos se encuentran indicados en el Anexo I.

9.4. Umbral para la registración y evaluación de las cuasi-pérdidas

- **Umbral para la registración de Cuasi – pérdidas:** Importe a partir del cual se registrarán las cuasi-pérdidas.
- **Umbral para la Evaluación de las cuasi-pérdidas:** Importe a partir del cual la Unidad de Riesgo Operacional deberá dar seguimiento a fin de solicitar algún plan de acción por parte de los dueños de los procesos. Los montos se encuentran indicados en el Anexo I.

X. PROCESO DE GESTIÓN DE RIESGO OPERACIONAL DEL BNF

10.1. Etapas del Proceso de Gestión del Riesgo Operacional

La institución ha establecido un proceso de Gestión de Riesgo Operacional, el cual abarca las siguientes etapas:

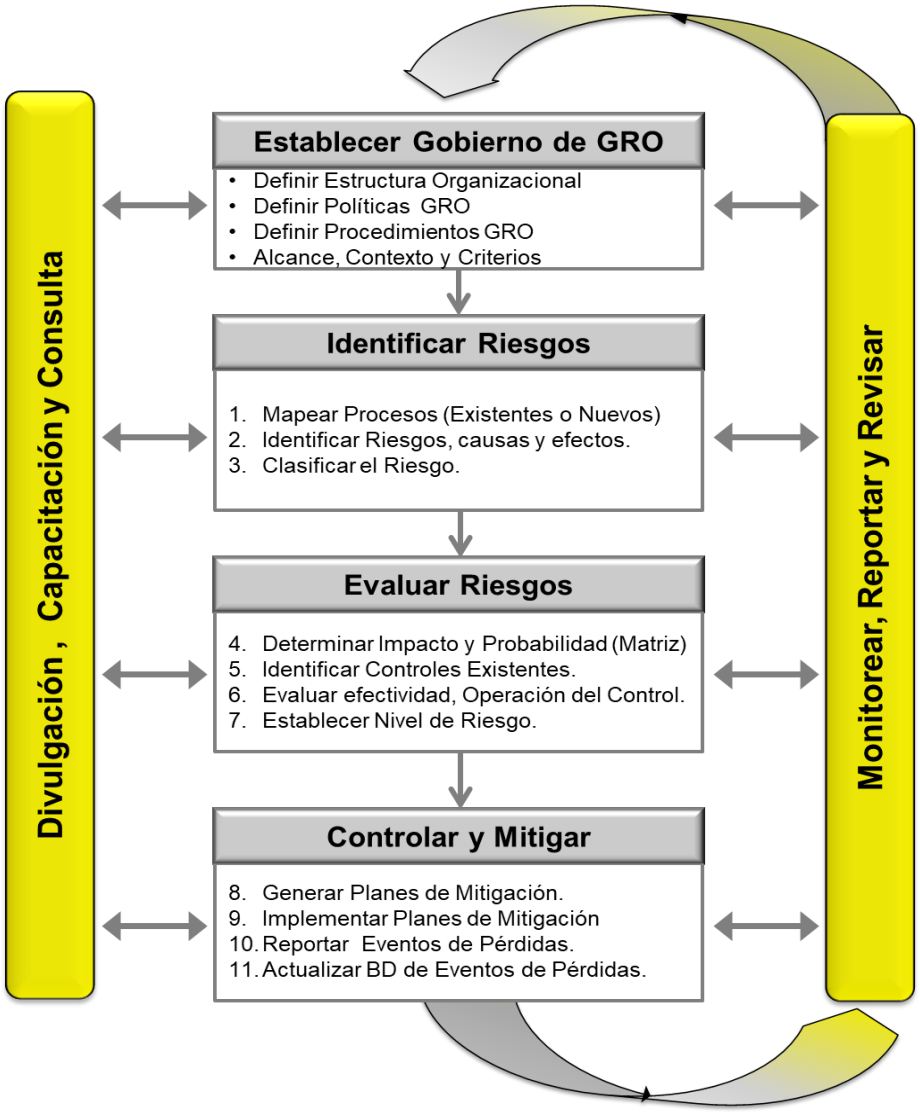

Figura 4: Etapas del Proceso de Gestión del RO

- **<u>Establecer Gobierno de GRO</u>:** Consiste en establecer la Gobernanza del Riesgo Operacional, en definir la estructura organizacional necesaria, que se encargará de diseñar y proponer las políticas, procedimientos, e implementar la metodología de gestión del riesgo operacional aprobadas.
- **<u>Identificar</u>**: Consiste en determinar los riesgos inherentes en todos los productos, actividades, procesos y sistemas importantes, teniendo en cuenta tanto factores internos (estructura de la institución, naturaleza de sus actividades, la calidad de los recursos humanos, cambios estructurales, rotación, entre otros), como factores externos (epidemia, pandemia, cambios en el sector y avances tecnológicos) que pudieran afectar el desarrollo de los procesos con un impacto negativo en las estrategias y por ende, en el logro de los objetivos de la institución.

Adicionalmente, dentro de esta etapa se deben identificar las fallas o insuficiencias de orden legal, a fin de determinar y comprender la exposición al riesgo legal que se encuentren asociadas al Riesgo Operacional.

Para poder puntualizar los riesgos, se debe partir de las actividades intrínsecas a los procesos o subprocesos establecidos por las Áreas (por lo que es indispensable contar con un completo mapeo de los procesos de la institución).

- **Evaluar**: Los riesgos inherentes identificados serán evaluados considerando su probabilidad de ocurrencia y su impacto en caso de materializarse. Estos riesgos serán evaluados con bases inherentes y bases residuales.

  Incluye la identificación de los controles establecidos como estrategia de limitación y control de riesgos, determinando su efectividad y su diseño.

  La institución debe asegurarse de evaluar los riesgos inherentes asociados a la introducción o emprendimiento de nuevos productos, actividades, procesos o sistemas nuevos y que los mismos sean sujetos a procedimientos adecuados de evaluación.

  Deberá realizar una efectiva evaluación del riesgo residual que permita entender el perfil del riesgo y asignar más efectivamente los recursos para la administración de los mismos.

  Otra herramienta que la entidad puede utilizar para identificar y evaluar sus riesgos operacionales es la utilización de Indicadores de Riesgos, que serán revisados con la periodicidad que se establezca, para monitorear sobre cambios que podría indicar un mayor riesgo, en cuyo caso podrá utilizar el procedimiento de **"Gestión y Monitoreo de Indicadores Clave de Riesgo Operacional".**

- **Controlar y Mitigar:** En esta etapa los Dueños de Procesos y/o los Gestores en coordinación con la Unidad de Riesgos Operacionales (URO) deberán analizar los riesgos y el tratamiento para evitarlos, aceptarlos, reducirlos o compartirlos, alineándolos con la tolerancia al riesgo definida por la entidad. De las acciones propuestas para reducir o transferir el nivel de riesgo residual se generarán los Planes de Mitigación.

  Asimismo, la institución contará con una Base de Datos actualizada para registrar los eventos de Riesgo Operacional que se pudieren presentar y que generen pérdidas o cuasi-perdidas, de manera a monitorear la materialización del riesgo previamente identificado.

  Como medidas de mitigación se podrán generar planes de contingencia y políticas de administración de riesgos por actividades externas relacionadas.

- **Monitorear, Reportar y Revisar:** En esta etapa se realiza el proceso de monitoreo regular del perfil de Riesgo Operacional, a los efectos de facilitar la rápida detección y corrección de las posibles deficiencias que se produzcan en los procesos y procedimientos de Gestión de Riesgo Operacional.

  Finalmente, la Unidad de Riesgo Operacional deberá remitir al Comité de Riesgo y a la Gerencia General periódicamente o cuando la situación lo amerite, informes vinculados a los resultados del seguimiento realizado y las pertinentes propuestas de corrección en los procesos y procedimientos, de manera que las autoridades puedan entender el perfil general de riesgo de la institución.

  Una vez analizados y aprobados los informes, se deberán distribuir al área afectada a fin de adoptar las medidas correctivas para asegurar una gestión eficaz del Riesgo Operacional.

  De acuerdo con las premisas de este modelo (proceso), los procedimientos formalizados y sus flujogramas juegan un rol importante en la implementación y continuidad del Riesgo Operacional, con lo cual recae la

responsabilidad de manera particular en cada uno de los Dueños de Procesos para identificar, medir, mitigar y monitorear los riesgos inherentes, así como proveer y mantener una comunicación efectiva entre cada área de la institución y la Unidad de Riesgo Operacional.

Las actividades que deben ser desarrolladas para cumplir con el proceso de evaluación de Riesgo Operacional se encuentran detalladas en el Manual de Procedimientos de Riesgo Operacional, en las secciones con la siguiente denominación:

- Procedimiento de "Identificación y Evaluación del Riesgo Operacional".
- Procedimiento de "Generación e Implementación de Planes de Mitigación".
- Procedimiento de "Actualización de Base de Datos de Eventos".
- Procedimiento de "Elaboración de Informes de Gestión y Seguimiento".

10.2. Valoración de Riesgos Inherentes

a) <u>Tabla de Frecuencia / Probabilidad de Materialización</u>: Se define como probabilidad, la posibilidad de que algo suceda, de la ocurrencia del evento o grupo de eventos que son evaluados, conforme a la tabla de frecuencia en el Anexo I – a) Tabla Impacto/Probabilidad.

b) <u>Tabla de Impacto</u>: Se define como el impacto, el resultado de la concreción de la ocurrencia de un evento o grupo de eventos, y que afecte el logro de objetivos del proceso o unidad de negocio en estudio, conforme a la escala definida y aprobada por el Directorio [Ver Anexo I: a) Tabla Impacto/Probabilidad].

10.3. Matriz de Riesgos

Una vez evaluados los riesgos de acuerdo con su frecuencia/probabilidad e impactos se debe construir la matriz de riesgos, con el objetivo de determinar el nivel de exposición, como se muestra en el siguiente gráfico:

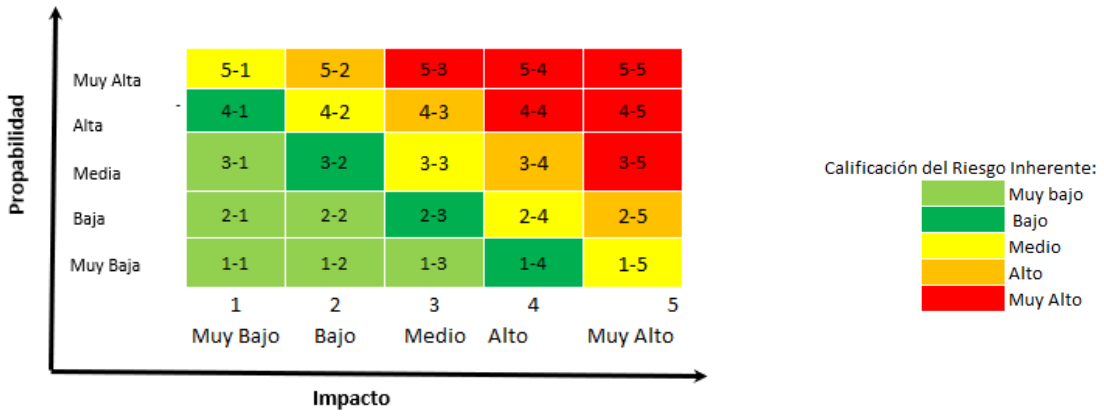

Figura 5: Matriz de Riesgo Inherente

10.4. Evaluación de los Controles

Los riesgos son mitigados con controles, los cuales deben ser evaluados de acuerdo con su efectividad y el diseño, siguiendo el siguiente criterio:

10.4.1 **Efectividad**

Escala	Calificación	Descripción
3	Fuerte	El control es muy adecuado, ya que cumple su función en forma eficiente (automático y preventivo).
2	Moderada	El control es adecuado; sin embargo, existen algunas debilidades que no representan un riesgo significativo (automático-detectivo o manual-preventivo).
1	Débil	El control no es adecuado, ya que no es de un nivel aceptable (manual y detectivo).

Tabla 1: Tabla Efectividad del Control.

10.4.2 **Diseño**

Escala	Calificación	Descripción
5	Muy Bueno	El control está diseñado para reducir al mínimo los efectos del riesgo. El proceso y el control se encuentra documentado y actualizado.
4	Bueno	El control está diseñado para reducir los principales efectos del riesgo. El proceso y el control se encuentran documentados, pero no actualizado.
3	Regular	El control está diseñado para reducir algún aspecto del riesgo. El proceso y algunos controles están documentados.
2	Malo	El control se halla mal diseñado, provee poca protección aun cuando está bien implementado. El proceso y el control no se encuentran documentados.
1	Muy Malo	El control está mal diseñado existe una ausencia de protección de la manera que está implementado. El proceso y el control no se encuentran documentados.

Tabla 2: Tabla Diseño del Control.

Derivado de la siguiente escala debe evaluar cuán importante es cada control para un riesgo, para lo cual deben adoptarse las siguientes definiciones:

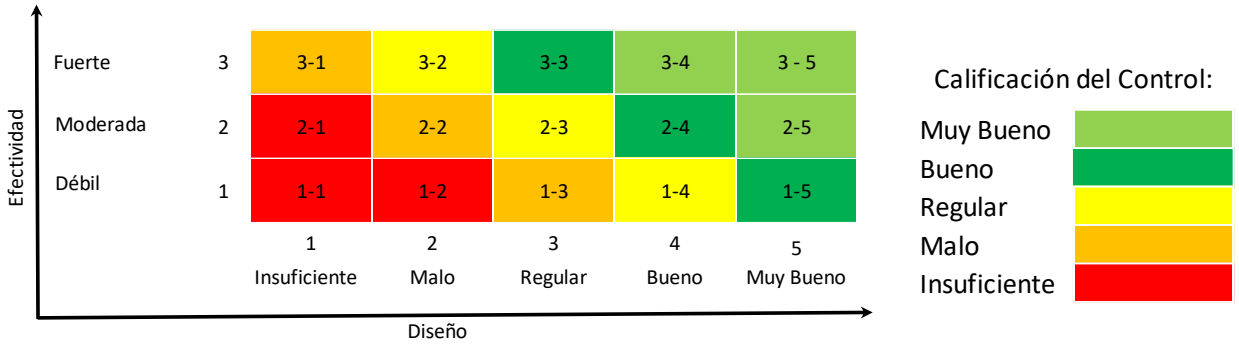

Figura 6: Matriz Evaluación del Control

10.5. Registro del Mapa de Riesgos

El diseño de un mapa de riesgos permite la visualización de los principales (pero no los únicos) riesgos que pueden afectar el cumplimiento de los objetivos institucionales y permite establecer medidas estratégicas para cuantificar, mitigar y monitorear los riesgos.

Como resultado de la valoración de los Riesgos en cuanto a probabilidad e impacto, y los controles en cuanto a efectividad y diseño, se obtiene el Mapa de Riesgos el cual contiene cómo mínimo: Código del Riesgo, Descripción del Riesgo Operacional, Clasificación del Evento, Calificación del Riesgo Inherente, Calificación del Control, Calificación del Riesgo Residual.

10.6. Matriz de Riesgo Residual

La Matriz de Riesgo Residual ubica cada uno de los eventos de Riesgo después de haber aplicado los controles, siguiendo el siguiente criterio:

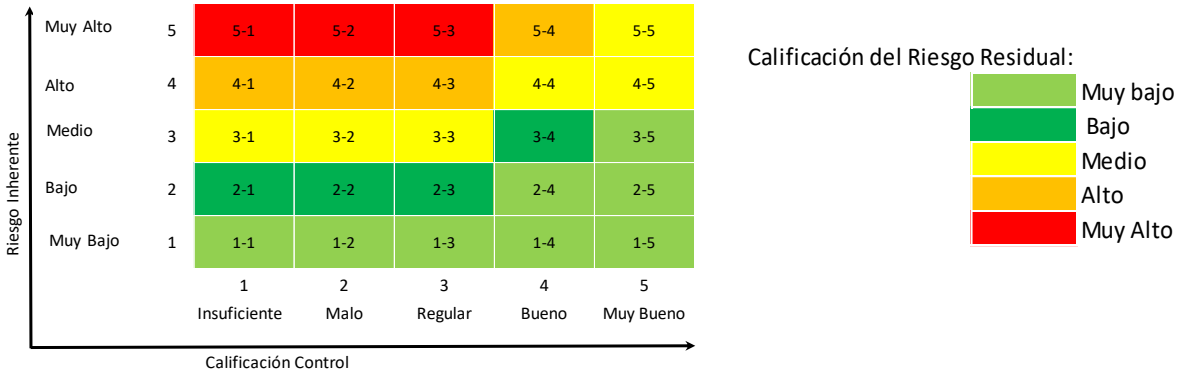

Figura 7: Matriz de Riesgo Residual

Una vez evaluados los controles, la metodología considera que dependiendo de la aplicación se podría reducir el riesgo. Algunos controles son fuertes reduciendo la probabilidad de ocurrencia del riesgo, el cual se reduciría únicamente si se cuenta con ellos.

Los controles ayudan a mitigar el riesgo junto con la automatización de operaciones, los planes de contingencia o traspaso del riesgo a un tercero, por ejemplo: seguros de daños, fianzas, etc.

10.7. Tratamiento del Riesgo

Las matrices de riesgos serán evaluadas en sesiones realizadas por el Dueño de Proceso y Gestores de RO en caso de requerir asistencia podrá intervenir la Unidad de Riesgo Operacional, con la finalidad de determinar cómo será administrado el riesgo y en qué casos se deberán establecer tratamientos tal como se muestra en el siguiente gráfico:

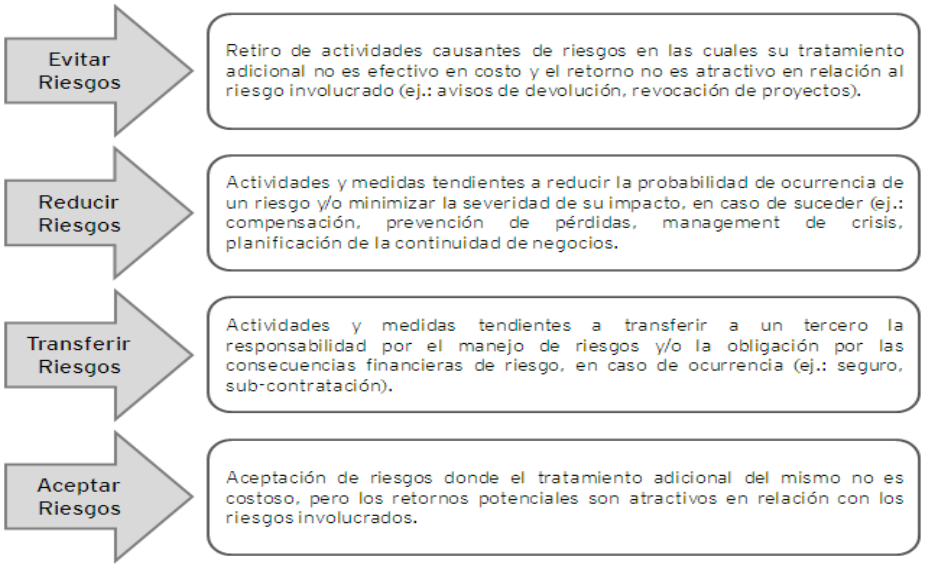

Figura 8: Tratamiento del Riesgo

De las decisiones que se adopten en las Sesiones de Trabajo, se deben desprender acciones correctivas dirigidas a las diferentes áreas de la institución de acuerdo con sus competencias y a los responsables de cada proceso con el fin de que los eventos más impactantes de riesgo residual se ubiquen en lugares de bajo impacto.

Las acciones correctivas serán incluidas en un Plan de Mitigación, que será ejecutado o implementado por las áreas de la institución responsables de sus procesos.

Como medidas de mitigación se podrán generar planes de contingencia y políticas de administración de riesgos por actividades externas relacionadas.

10.8. Monitoreo del Perfil de Riesgo

El apetito al riesgo se compara con el perfil de riesgo, que es la posición de riesgo de la Entidad en un momento dado considerando todos sus riesgos identificados (consolidado de matrices de evaluación de riesgos), y con la tolerancia al riesgo, que es el nivel máximo de riesgo que una entidad puede asumir al realizar su actividad.

Las actividades para llevar a cabo el monitoreo del perfil de Riesgo del BNF se encuentran detalladas en el Manual de Procedimientos de Riesgo Operacional, en la sección denominada:

- Procedimiento “Análisis del perfil de riesgo operacional”.

10.9. Registro de Eventos de Riesgo

El BNF cuenta con una Base de Datos para registrar los eventos de Riesgo Operacional que se pudieren presentar y que generen pérdidas y afecten el Estado de Resultados de la institución. Así como Eventos que no resultan en una pérdida financiera (cuasi-perdidas).

La Base de Datos contiene la siguiente información:

a. Identificación, tipo y descripción del evento.
b. Fecha de descubrimiento, de ocurrencia o de inicio del evento.
c. Fecha de Registro Contable del evento de pérdida.
d. Cuantificación de la pérdida.
e. Monto recuperado (Parcial o Total), mediante coberturas existentes.
f. Cobertura con Póliza de Seguro.
g. Identificación de su vinculación con otros riesgos.

Los criterios para el registro de los eventos de riesgo operacional se encuentran definidos en el Manual de Procedimientos de Riesgo Operacional, en la sección denominada:

- Procedimiento de “Actualización de Base de Datos de Eventos"

XI. INFORMES GERENCIALES

La División Riesgos Operativos que forma parte de la URO; debe elaborar los informes conforme el *Esquema de Periodicidad de Informes* descrito en el Procedimiento “Elaboración de Informes de Gestión y Seguimiento” y elevar a la Gerencia Departamental de Riesgo Integral, a la Gerencia de Área de Riesgos, al Comité de Riesgos, la Gerencia General y éste último al Directorio, a fin de dar cumplimiento a los reportes sobre el avance en la implementación del Sistema de Gestión de Riesgo Operacional y aquellos que en el futuro establezca la Superintendencia de Bancos del Paraguay.

La Unidad de Auditoria Interna debe informar los resultados de las evaluaciones sobre la efectividad y el cumplimiento de las etapas de la Metodología de Gestión de Riesgo Operacional, informes que debe presentar, en forma preliminar a la Unidad de Riesgo Operacional, y en forma final al Comité de Auditoría, a Gerencia General y al Directorio.

XII. DIVULGACIÓN Y CAPACITACIÓN

La Unidad de Riesgo Operacional coordinará con las áreas de la institución que correspondan, actividades necesarias para asegurar que la información concerniente a la Metodología de Gestión de Riesgo Operacional sea divulgada en forma periódica y adecuadamente, reflejadas en algún informe de gestión de la institución como ser: Informe de Gobierno Corporativo, Memoria Institucional o Página Web, entre otros, que la institución considere pertinente.

Además, la institución deberá divulgar información suficiente sobre sus políticas, procesos y procedimientos relacionados a la gestión de Riesgo Operacional, para que terceras personas puedan evaluar el enfoque utilizado por la institución en este aspecto.

La capacitación se realizará por lo menos una vez al año, y deberá hacer parte también del proceso de inducción de la institución y ser objeto de evaluación para eficacia frente a las políticas y objetivos del sistema. Para el efecto la Unidad de Riesgo Operacional presentará un Esquema de Capacitación Anual al Comité de Riesgos para su aprobación, de acuerdo con los lineamientos establecidos en las ***Políticas de Talento Humano*** relacionados a la Capacitación del personal del BNF.

Los Materiales de Capacitación deben ser actualizados y la ejecución del Esquema deberá ser permanente y constante, a los efectos de su actualización para los funcionarios, ya sea a través de recordatorios, evaluaciones-test concientizando a todo el personal de la importancia de los riesgos.

XIII. AUDITORÍA INTERNA

La Gerencia de Área de Auditoria Interna debe llevar a cabo revisiones anuales dentro de su Plan Anual de Auditoría Interna, en el marco de la gestión del Riesgo Operacional, comprobar el cumplimiento y evaluar la eficacia de las políticas y procedimientos establecidos para este fin, y realizar los informes y las recomendaciones que deriven de su evaluación.

La Gerencia de Área de Auditoria Interna debe informar los resultados de las evaluaciones sobre la efectividad y el cumplimiento de las etapas del SARO, informes que debe presentar, en forma preliminar a la Unidad de Riesgo Operacional, y en forma final al Comité de Auditoría, a Gerencia General y al Directorio.

XIV. REVISIÓN DEL MANUAL

La documentación deberá ser revisada con una periodicidad mínima de un año o cada vez que la Alta Gerencia lo estime oportuno y conveniente de acuerdo con los resultados obtenidos de su aplicación, ante hechos o situaciones de relevancia vinculadas a este riesgo y de acuerdo con las disposiciones legales vigentes al respecto.

En caso de que el manual no sufriera modificación o cambios, como parte del proceso de revisión anual se deberá informar al Comité de Riesgos de la revisión y dejar registrado en actas, como evidencia de revisión.

ANEXO I

a) Tabla de Impacto/ Probabilidad

1) La Alta Dirección de la institución, ha determinado la siguiente escala de impacto (cuantitativo), calculado sobre el 0,1% del Patrimonio Efectivo anual:

Escala	Calificación	Descripción	Impacto Económico
5	Muy Alto	Riesgos extremadamente severos los cuales conllevan a una pérdida monetaria desastrosa que puede llevar a la pérdida de ingresos o afectar totalmente el patrimonio del banco, puede llegar a provocar interrupción de las operaciones de la institución.	mayor a Gs. 1.718.167.743
4	Alto	Fuerte efecto monetario por eventos derivados de un riesgo severo que puede llegar a provocar interrupción de una parte de las operaciones de la institución.	Mayor a Gs. 876.265.547 hasta Gs. 1.718.167.743
3	Medio	Efecto monetario moderado derivado de una contingencia produciendo inconvenientes moderados.	Mayor a Gs. 343.633.549 hasta Gs. 876.265.547
2	Bajo	Efecto monetario mínimo derivado de una posible contingencia que puede producir o generar leves inconvenientes.	Entre Gs. 120.271.741 hasta Gs. 343.633.549
1	Muy Bajo	Efecto mínimo derivado de riesgos que no afectan la productividad de la institución, pueden o no producir o generar inconvenientes menores.	Menor a Gs. 120.271.742

Tabla 1: Tabla de Impacto

2) Así mismo se determinó la siguiente escala de Probabilidad/Frecuencia:

En la determinación de la frecuencia no se deben tener en consideración los controles o mitigantes asociados:

Escala	Calificación	Frecuencia	Descripción
5	Muy Ata	1 o más veces al mes	Se espera que el evento ocurra, con muy alta probabilidad de ocurrencia o se ha materializado una o más veces en el último mes.
4	Alta	varias veces en el mismo año	El evento es muy probable que ocurra, alta probabilidad de ocurrencia o ha ocurrido varias veces en el mismo año.
3	Media	1 vez cada 1 año	El evento es probable que ocurra, mediana probabilidad de ocurrencia o se ha materializado una vez en el último año.
2	Baja	1 vez cada 3 años	El evento es poco probable que ocurra, baja probabilidad de ocurrencia ha ocurrido en los últimos 3 años o más.
1	Muy Baja	1 vez cada 5 años	El evento es poco probable que ocurra, baja probabilidad de ocurrencia ha ocurrido en los últimos 5 años o más.

Tabla 2: Tabla de Probabilidad

b) Definición de Umbrales

El Directorio del BNF determinó como tolerancia máxima o **Monto Máximo de Pérdidas Totales** por **eventos de perdida por riesgo operacional** registrados en un ejercicio fiscal, el **0,1%** del Patrimonio Efectivo (PE) de la institución en el ejercicio fiscal del año anterior. En la tabla 3, se encuentra definido el Monto Máximo estimado en función del Patrimonio Efectivo del BNF en el ejercicio fiscal diciembre 2019.

En caso de que el nivel de riesgo observado exceda el umbral autorizado por el Directorio; la División Riesgos Operativos inmediatamente después de haberlo detectado, deberá investigar y documentar en conjunto con las áreas involucradas, las causas que originaron las desviaciones al umbral establecido e informará a la Gerencia Departamental de Riesgo Integral y a la Gerencia de Área de Riesgos de la desviación; luego se elevará al Comité de Riesgos para su conocimiento y tratamiento respectivo.

La División Riesgos Operativos deberá identificar si dichas desviaciones se presentan en forma reiterada e informar de manera oportuna los resultados al Comité de Riesgos.

Por otro lado, la registración, el seguimiento y la evaluación eventos de pérdidas y de cuasi pérdidas se realizarán, según la siguiente escala en la Tabla 3, definida por el Directorio, en concordancia con la tabla de Impacto económico, basada en el 0,1% del Patrimonio Efectivo de la institución en el ejercicio del año anterior:

	Umbrales	Criterios de Registros	Monto
Nivel de Tolerancia Global	Nivel Monto Máximo de Pérdidas Totales	0.1% del PE	GS. 1.718.167.743
Pérdidas Financieros	Umbral para registración de eventos por pérdida de RO-	Importe desde el cual se realiza el registro de eventos de pérdida en la base de datos	De Gs.1,-
	Umbral para seguimiento de pérdidas de riesgo operacional	Importe desde el cual se realiza el seguimiento de eventos de pérdida. Hasta que monto Gestores de RO, desde que monto la URO	Dueños de Procesos y Gestores RO desde Gs. 1 hasta Gs. 125.000.000. URO realiza el acompañamiento y monitoreo al seguimiento realizado por Dueños de Procesos y Gestores RO por encima de Gs. 125.000.000
Cuasi-pérdidas	Umbral para registración de cuasi-pérdidas	Monto desde el cual se registran las cuasi-perdidas	De Gs.1
	Umbral para seguimiento de cuasi-pérdidas	A partir de dicho valor se necesita dar seguimiento al evento por parte del Dueño del Proceso y elevar los resultados del mismo a la URO.	Dueños de Procesos/Gestores de RO desde Gs. 1 hasta 250.000.000, - Uro realiza el acompañamiento y monitoreo al seguimiento realizado por Dueños de Procesos y Gestores RO por encima de Gs. 250.000.000,

Tabla 3: Umbrales de RO