METODOLOGÍA DE GESTIÓN INTEGRAL DE RIESGOS

TABLA DE CONTENIDO

I. INTRODUCCIÓN 3
II. OBJETIVOS 3
III. ALCANCE 3
IV. DEFINICIONES 3
4.1. Riesgo 4
4.2. Apetito por el Riesgo 4
4.3. Control 4
4.4. Declaración del Apetito por el Riesgo 4
4.5. Evento 4
4.6. Gestión del Riesgo 4
4.7. Límites de Riesgo: 4
4.8. Impacto 4
4.9. Marco de Gestión de Riesgo 4
4.10. Perfil de Riesgo 5
4.11. Probabilidad 5
4.12. Propietario/ Dueño del riesgo 5
4.13. Tolerancia al Riesgo 5
4.14. Umbral 5
4.15. Monitoreo 5
V. ENFOQUE DE INTEGRACIÓN 5
VI. GOBERNANZA DEL RIESGO 6
VII. ESTRATEGIA DE RIESGOS 7
VIII. DOCUMENTACIÓN, ROLES, RESPONSABILIDADES Y AUTORIDADES 7
IX. CATEGORIAS DE RIESGOS 10
X. PROCESO DE GESTIÓN DE RIESGOS 10
1. Alcance, contexto y criterios de Riesgos 12
2. Identificación de Riesgos 15
3. Análisis del riesgo 16
4. Evaluación del riesgo 16
5. Tratamiento del riesgo 16

6. Seguimiento y Revisión....17
7. Comunicación y Consulta....17
8. Documentación y Reportes....18
XI. ANEXOS....18

I. INTRODUCCIÓN

El Directorio del **BANCO NACIONAL DE FOMENTO** (en adelante **BNF**) ha venido trabajando en el fortalecimiento de sus estructuras de Gobierno Corporativo, promoviendo una cultura de riesgos en la organización.

El Directorio de **BNF** en consonancia a lo establecido por las disposiciones emanadas de entes reguladores locales, así como también en adopción de prácticas bancarias prudentes y recomendaciones referidas por organismos internacionales, tal como lo son el "Comité de Supervisión Bancaria de Basilea" y la Organización Internacional de Normalización (ISO) formaliza a través del presente documento la metodología de Gestión Integral de Riesgos.

El marco de gobierno del riesgo del **BNF** incluye e implica la aplicación sistemática de políticas, procedimientos y mejores prácticas para la administración de los riesgos a nivel integral en la institución, en forma proporcional a su tamaño y complejidad de operaciones.

II. OBJETIVOS

Definir y estandarizar la metodología a seguir para gestionar los riesgos y oportunidades de diferentes ámbitos de gestión asociados a los procesos de la Institución.

La gestión de riesgos:

- Debe ser utilizada como herramienta para la toma de decisiones de gestión y de negocios.
- Debe ayudar a gestionar los cambios que la institución pueda sufrir.
- Debe contar con la mejor información disponible, lo que significa que los elementos de entrada al proceso de gestión del riesgo se han de basar en fuentes de información fiables tales como datos históricos, experiencia, retroalimentación de las partes interesadas, observación, previsiones y juicios de expertos, así como con adecuados elementos de salida que permitan el logro de los resultados previstos y con ello la mejora de los procesos.

Esto es, la gestión sistemática del riesgo debe ayudar a tomar mejores decisiones, estableciendo y logrando los objetivos y mejorando el desempeño.

III. ALCANCE

El enfoque metodológico del presente documento es aplicable a todos los procesos y a todos los funcionarios del **BANCO NACIONAL DE FOMENTO**, y es aplicable a todos los tipos de riesgos y a la toma de decisiones en todos los niveles de la institución.

Este documento ha sido elaborado tomando como marcos de referencia la norma ISO 31000:2018 Gestión del Riesgo - Directrices y los Principios de Gobierno Corporativo para bancos, Basilea III.

IV. DEFINICIONES

Los términos clave dentro de esta metodología a continuación:

4.1. Riesgo

El efecto de la incertidumbre sobre los objetivos[1].

4.2. Apetito por el Riesgo

Nivel agregado y tipos de riesgo que un banco está dispuesto a asumir en su búsqueda de la rentabilidad, previamente decidido y dentro de su capacidad de riesgo, a fin de lograr sus objetivos estratégicos y plan de negocio.

4.3. Control

Medida que mantiene y/o modifica el riesgo. Los controles incluyen, pero no se limitan a: cualquier proceso, política, dispositivo, prácticas u otras acciones que mantienen y/o modifican el riesgo.

4.4. Declaración del Apetito por el Riesgo

Articulación escrita del nivel agregado y los tipos de riesgo que el banco aceptará, o evitará, a fin de lograr sus objetivos de negocio. Incluye medidas cuantitativas expresadas en términos relativos de beneficios, capital, medidas de riesgo, liquidez y otras medidas relevantes según proceda.

4.5. Evento

Ocurrencia o cambio de un conjunto de circunstancias. Un evento puede tener una o más ocurrencias y puede tener varias causas o varias consecuencias. Un evento puede ser algo previsto que no llega a ocurrir, o algo no previsto que ocurre.

4.6. Gestión del Riesgo

Procesos establecidos para garantizar que todos los riesgos materiales y sus correspondientes concentraciones de riesgo se identifican, miden/analizan, limitan, controlan, mitigan/tratan y notifican/informan de forma oportuna e íntegra[2].

4.7. Límites de Riesgo:

Medidas o límites cuantitativos específicos basados en, por ejemplo, supuestos prospectivos que asignan el riesgo agregado de la entidad a las líneas de negocio, entidades jurídicas relevantes, categorías de riesgo específicas, concentraciones u otras medidas pertinentes.

4.8. Impacto

El resultado de que un evento o grupo de eventos afecte los objetivos.
Una consecuencia puede ser cierta o incierta y puede tener efectos positivos o negativo, directos o indirectos sobre los objetivos. Las consecuencias se pueden expresar de manera cualitativa o cuantitativa.

4.9. Marco de Gestión de Riesgo

Actividades coordinadas para dirigir y controlar la organización con relación al riesgo[3].

[1] ISO 31000:2018

[2] Principios de gobierno corporativo para bancos, Basilea, 2015.
[3] ISO 31000:2018

4.10. Perfil de Riesgo

Valoración en un momento dado de las exposiciones al riesgo netas (es decir, tras aplicar atenuantes) agregadas dentro de y a través de cada categoría de riesgo relevante a partir de supuestos actuales o prospectivos.

4.11. Probabilidad

Posibilidad de que algo suceda.
Esté definida, medida o determinada objetiva o subjetivamente, cualitativa o cuantitativamente y descrita utilizando términos generales o matemáticos.

4.12. Propietario/ Dueño del riesgo

Persona, área, unidad o entidad con responsabilidad y autoridad para gestionar un riesgo.

4.13. Tolerancia al Riesgo

Consiste en el nivel aceptable de variación en los resultados o actuaciones de la entidad, relativas a la consecución o logro de sus objetivos.

4.14. 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.

4.15. Monitoreo

Verificación continua, supervisión, observación crítica o determinación del estado para identificar cambios en el nivel de rendimiento requerido o esperado.

Un riesgo sin gestionar, aceptar o mitigarse completamente, normalmente se convierte en un problema.

V. ENFOQUE DE INTEGRACIÓN

Las actividades por llevar a cabo por el Proceso de Gestión de Riesgo están integradas con los requisitos de las diferentes normas ISO, dentro del alcance de las cláusulas:

4.1 Comprensión de la organización y de su contexto.

4.2 Comprensión de las necesidades y expectativas de las partes interesadas.

6.1 Acciones para abordar riesgos y oportunidades.

Se ha de llevar a cabo un proceso de comunicación y un proceso de seguimiento continuo durante todo el proceso.

Asimismo, las actividades del proceso de gestión de riesgo descritas en la sección "***Proceso de Gestión de Riesgos***" están integradas con los principios de Gobierno Corporativo para bancos, del "Comité de Supervisión Bancaria de Basilea", dentro del alcance de:

Principio 6: Función de gestión del riesgo.

Principio 7: Identificación, seguimiento y control de riesgos

Principio 8: Comunicación de riesgos

Principio 12: Divulgación y transparencia

VI. GOBERNANZA DEL RIESGO

La responsabilidad de la gestión del riesgo para administrar las actividades en el **BNF**, se asignan utilizando las tres líneas de defensa (Se puede observar gráficamente en la Figura 1: Tres Líneas de Defensa del BNF):

1. Primera Línea: Unidades de Negocio, quienes son propietarios/ dueños de los riesgos y controles.
2. Segunda Línea: Función de Gestión del Riesgo Independiente y Función de Cumplimiento Normativo Independiente, quienes proveen el Marco Metodológico, Políticas, seguimiento y monitoreo del cumplimiento.
3. Tercera Línea: Auditoría (función de auditoría interna, auditoría externa), que provee auditoría y evaluación de cumplimiento independiente.

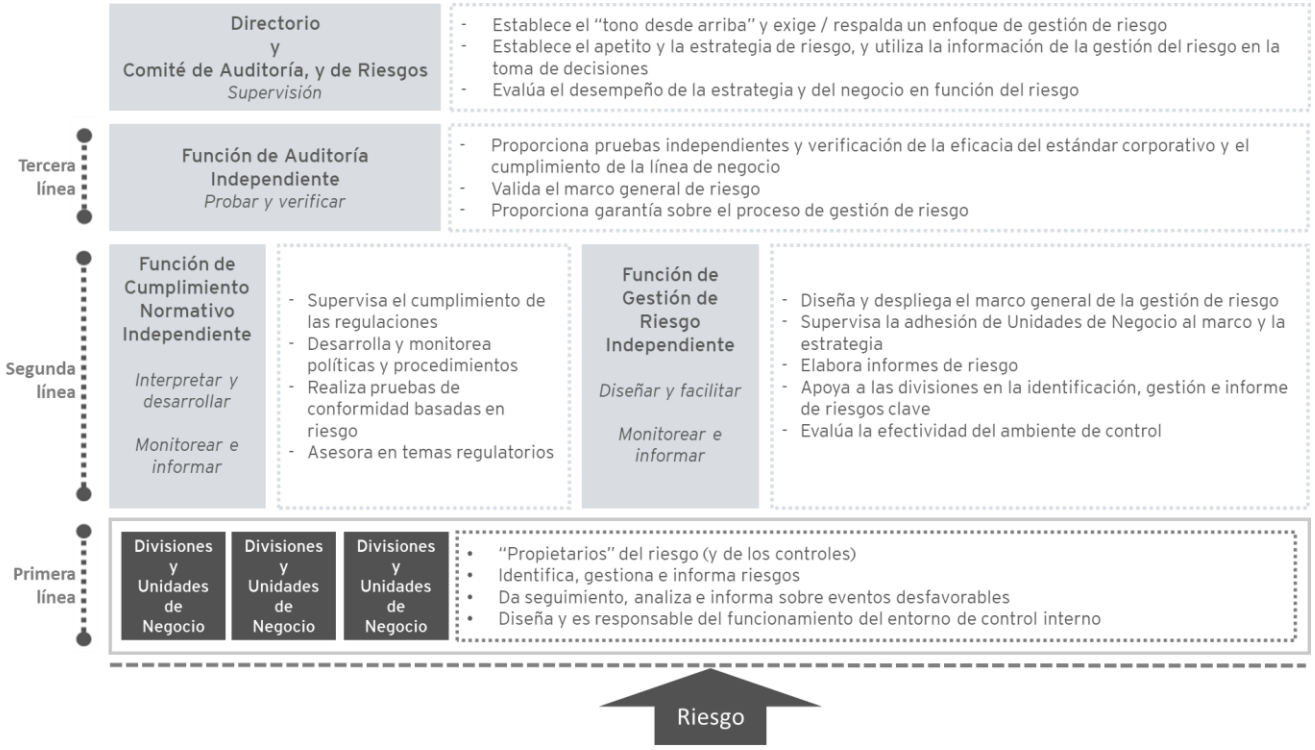

Figura 1: Tres Líneas de Defensa del BNF

VII. ESTRATEGIA DE RIESGOS

El **BNF** ha adoptado una estrategia de riesgos que incluye los tipos o categorías de riesgos que el Banco quiere asumir en forma activa, que se describe en el **Anexo 1 – Estrategia de Gestión de Riesgos**.

El Apetito al riesgo del **BNF** está definido por los tipos de riesgos (categorías) que el banco está dispuesto a asumir en su búsqueda de la rentabilidad, dentro de su capacidad de riesgo, a fin de lograr sus objetivos estratégicos y plan de negocio. La articulación escrita del nivel de riesgo que el banco aceptará o evitará se encuentra en el **Anexo 2- Declaración del Apetito de Riesgos.**

VIII. DOCUMENTACIÓN, ROLES, RESPONSABILIDADES Y AUTORIDADES

Los roles y responsabilidades para la gestión de riesgos en el **BNF** se han estructurado para lograr que el Directorio se comprometa a establecer "el tono" o intensidad para la gestión del riesgo desde arriba, y con el asesoramiento de la función del riesgo, permear en cascada la cultura de gestión de riesgos a toda la organización. Por tanto, toda la dirección y el personal deben conocer y estar comprometidos en cumplir sus responsabilidades de gestión de riesgos.

La entidad cuenta en su estructura organizacional con una unidad de gestión integral de riesgos cuya dependencia orgánica y funcional responde a la Gerencia General, bajo la dirección de un Gerente de Área de Riesgos, con suficiente autoridad, independencia, recursos y acceso al Directorio.

Los roles y responsabilidades para la implantación de la gestión integral de riesgos en BNF, que se encuentran definidos en la siguiente tabla, complementan el Manual de Organización y Funciones del BNF (cuando aplique).

Rol	Responsabilidades
Directorio	▶ Aprobar el **Marco de Gestión Integral de Riesgos** que deberá garantizar que la gestión está integrada en todas las actividades de la institución. ▶ Establecer la magnitud y el tipo de riesgos que puede o no ser tomado para guiar el desarrollo de los criterios del riesgo, asegurando que se comunican a la institución y sus partes interesadas. ▶ Aprobar los roles y responsabilidades relacionadas a la gestión integral de riesgos y que corresponden a los diferentes niveles de la institución. ▶ Asegurar que están disponibles los recursos necesarios para la gestión integral de riesgos. ▶ Tener un claro conocimiento sobre el perfil de Riesgo de la Institución y verificar sus implicancias en el alcance de los objetivos estratégicos. ▶ Asegurar que la gestión de riesgos esté sujeto a un órgano de supervisión y sea eficaz e integral.
Gerencia General	▶ Determinar el Alcance de la Gestión Integral de Riesgos. ▶ Aprobar los Planes de Implementación del Tratamiento del Riesgo y la Aceptación del Riesgo. ▶ Asignar autoridad y responsabilidad en los niveles apropiados de la organización. ▶ Comunicar la importancia de una gestión integral de Riesgos en toda la Institución. ▶ Tener un claro conocimiento sobre la gestión del Riesgo, su grado de cumplimiento, verificando su implicancia en el alcance de los objetivos estratégicos, para ello, deberá recibir información con una periodicidad adecuada, e informar suficiente sobre el perfil de Riesgo de la Institución al **Directorio**. ▶ Revisar informes de auditarías internas y promover la mejora continua.

Rol	Responsabilidades
Comité de Riesgos	▶ Las funciones del Comité de Riesgos se encuentran en su correspondiente Manual de Organización y Funciones del BNF.
Gerente de Área de Riesgos (CRO)[4]	▶ Gestionar el diseño, la implementación, la evaluación constante y la mejora continua de la Gestión Integral de Riesgos. ▶ Desarrollar el **Marco de Gestión de Riesgos,** que incluya la cultura del riesgo del banco, su apetito y límites por el riesgo. ▶ Desarrollar el Plan de Trabajo de la Gestión de Riesgos. ▶ Proponer al Comité la asignación de roles y responsabilidades relacionados a la gestión integral de riesgos, desarrollado en coordinación con **Talento Humano**. ▶ Asesorar a las **Divisiones y Unidades de Negocio** en la identificación, evaluación, tratamiento registro e informe de riesgos. ▶ Determinar las competencias necesarias de las personas que operan la Función de Gestión de Riesgo independiente. ▶ Desarrollar, someter a aprobación e implementar el Plan de Comunicación y Concienciación del Riesgo. ▶ Elaborar los informes sobre la Gestión Integral del Riesgo y elevarlos al **Comité de Riesgos.** ▶ Revisar la efectividad de mitigación de riesgo de los planes implementados, solicitar acciones correctivas donde sea aplicable. ▶ Evaluar la efectividad y la eficiencia de la gestión del riesgo seleccionada y el cumplimiento interno en toda la institución.
Gerencia Departamental de Gestión de Riesgo Integral	▶ Apoyar en el desarrollo del **Marco de Gestión de Riesgos**. ▶ Desarrollar el Plan de Trabajo de la Gestión de Riesgos de su unidad organizacional. ▶ Supervisar y asesorar al equipo de Gestión de Riesgos (Dueños/ Líder de Procesos, Aliados/Gestores). ▶ Apoyar en el desarrollo del Plan de Comunicación y Concienciación del Riesgo. ▶ Llevar los registros y apoyar en la consolidación de los informes sobre la Gestión Integral del Riesgo. ▶ Proponer alternativas para la mitigación y control de los riesgos. ▶ Supervisar el rendimiento proceso de evaluación de riesgo frente a las proyecciones iniciales y de acuerdo a los resultados asegurar la adaptación de tratamiento conforme madura el negocio.
Asistente de Gestión Integral de Riesgo	▶ Apoyar en la mejora de los sistemas de gestión del riesgo y su correspondiente documentación. ▶ Mantener un registro de las acciones de Comunicación, Concienciación y capacitaciones dictadas al personal y de materiales utilizados en los mismos en materia de Gestión Integral de Riesgos. ▶ Recibir y analizar información relativa a la gestión de riesgo del banco y a los resultados frente a la asunción de riesgos. ▶ Consolidar los informes relativos a la gestión de cada riesgo y someter a aprobación del **Gerencia Departamental de Gestión de Riesgo Integral.** ▶ Mantener informado al Gerente Departamental de Gestión de Riesgo Integral respecto a las actividades y novedades de su sector; y realizar las consultas que fueren necesarias en el momento oportuno. ▶ Mantener un registro ordenado y adecuado de las documentaciones relacionadas con su área.

[4] Chief Risk Officer

Rol	Responsabilidades
Líder/Dueño de Procesos / Propietario de Riesgos	Es Responsable de la aplicación sistemática de políticas, procedimientos, esta metodología y prácticas en la estructura, las operaciones y procesos del cual es dueño. Puede aplicarlas a nivel estratégico, operacional, de programa o de proyecto. Para ello deberá: ▶ Participar en las sesiones de evaluación del Riesgo, cuando sea necesario. ▶ Aprobar el resultado del análisis de riesgos, realizado por el **Aliado/Gestor** designado para el proceso del cual es dueño. ▶ Definir e implementar los planes de acción/mitigación. ▶ Proporcionar información relacionada con el seguimiento de las acciones referentes a los planes de acción/mitigación. ▶ Reportar los eventos de riesgos registrados en los procesos (de los cuales es dueño), al momento de la toma de conocimiento de su ocurrencia. ▶ Implementar, aplicar, mantener y actualizar los Controles, cuyas acciones preventivas y correctivas, permitirán la mitigación de los riesgos. ▶ Mantener una estrecha comunicación con su unidad organizacional, así como con el **Área de Riesgos**, con relación al riesgo que esté gestionando y contribuir a una mejora continua. ▶ Fomentar en su unidad organizacional una cultura donde los riesgos son identificados y escalados. ▶ Comunicar cualquier cambio sustancial del proceso (del cual es dueño), al **Gerente de Planificación y Desarrollo** con copia al **Gerente de Área de Riesgos**.
Aliados/ Gestores de la Gestión del Riesgo	Es la persona designada por el **Líder/Dueño del Proceso**, como responsable de la identificación, evaluación y registro de riesgos en los formularios correspondientes, para ello deberá. ▶ Identificar y evaluar los riesgos. Determinar las causas y efectos derivados a los riesgos identificados. ▶ Identificar si el riesgo es cuantificable y si provoca una pérdida directa o indirecta para la Institución. ▶ Determinar, cada vez que sea identificado un riesgo, la probabilidad (frecuencia) e impacto (consecuencia) para aquellos riesgos cuantificables o no por pérdidas directas. ▶ Identificar y evaluar los controles del proceso crítico evaluado. ▶ Proponer planes de acción/mitigación. ▶ Reportar los eventos de pérdidas registrados en su unidad organizacional por los canales establecidos, al momento de la toma de conocimiento de su ocurrencia. ▶ Realizar reporte de riesgos en nombre de su unidad organizacional (cuando sea responsable de la supervisión de la gestión de un tipo de riesgo) y someter a aprobación del **Dueño de Proceso**. ▶ Educar a las partes interesadas que se encuentran dentro del ámbito de su influencia sobre las prácticas de gestión de riesgo.
Auditoría Interna	▶ Planificar las auditorías internas de Gestión Integral de Riesgos. ▶ Ejecutar la auditoría interna. ▶ Presentar Informe de Auditoría Interna al **Directorio**. ▶ Hacer seguimiento de las recomendaciones y/u oportunidad de mejora.
Talento Humano	▶ En coordinación con el **Gerente General,** trabajar para mantener la estructura adecuada de Gestión de Riesgos. ▶ Trabajar en coordinación con el **Gerente de Área de Riesgos** en la asignación de roles y responsabilidades relacionadas a la gestión integral de riesgos.

Rol	Responsabilidades
Todos los empleados	▶ Comprometerse y cumplir con las políticas, metodología y procedimientos de gestión de riesgos. ▶ Identificar, analizar y reportar riesgos significativos del negocio en las actividades realizadas.

IX. CATEGORIAS DE RIESGOS

Las categorías de riesgo describen grupos de riesgo específico que se relaciona a todo el banco. Definir estas categorías permite al **BNF** una comparación consistente de riesgo en toda la institución.

Todos los funcionarios deben reconocer que cada decisión que toman, cada acción que llevan a cabo tiene un impacto en la institución en términos:

- **Riesgo Ambiental y Social**: Riesgo que pueden impactar en el funcionamiento del medio ambiente y ecosistema en el corto y largo plazo, y riesgos que pueden impactar en áreas o ítems de importancia cultural.
- **Riesgo Crediticio**: Riesgos relacionados al análisis y evaluación de concesión de créditos.
- **Riesgo de Lavado de Dinero**: Riesgo relacionado a que el BNF pueda ser utilizado como instrumento para lavar activos o como canal de recursos para promover actividades terroristas
- **Riesgo de TI**: Riesgo relacionado a los servicios de TI y programas de trabajo de TI.
- **Riesgo del Personal**: Riesgo relacionado a la retención y capacidad de los funcionarios y subcontratados.
- **Riesgo Estratégico**: Riesgo que puede impactar en el alcance de los objetivos estratégicos del BNF.
- **Riesgo Financiero**: Riesgo de mercado y de liquidez, relacionado a las pérdidas en posiciones, derivadas de movimientos en los precios de mercado y la posibilidad de pérdida financiera por incumplir con los requerimientos de financiamiento y de aplicación de fondos que surgen de los descalces de flujos de efectivo.
- **Riesgo Legal**: Riesgos relacionados al cumplimiento legal y regulatorio.
- **Riesgo Operacional**: Riesgo relacionado a los procesos, personas y sistemas de la institución. Así como riesgos relacionados a factores externos que pueden impactar en la continuidad del negocio.
- **Riesgo Reputacional**: Riesgos relacionados a la percepción y confianza del público hacia la institución.
- **Riesgo Salud y Seguridad**: Riesgo relacionado a la salud y seguridad de los funcionarios del BNF y el público en general. Riesgo relacionado a daños en la infraestructura que pueda afectar el acceso de las unidades de negocios a su sito de trabajo.

X. PROCESO DE GESTIÓN DE RIESGOS

El proceso de gestión de riesgos implica la aplicación sistemática de políticas, procedimientos y mejores prácticas a las actividades de comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registro e informe del Riesgo.

El **BNF** adopta un proceso de gestión integral de riesgos que se ilustra en la figura 2.

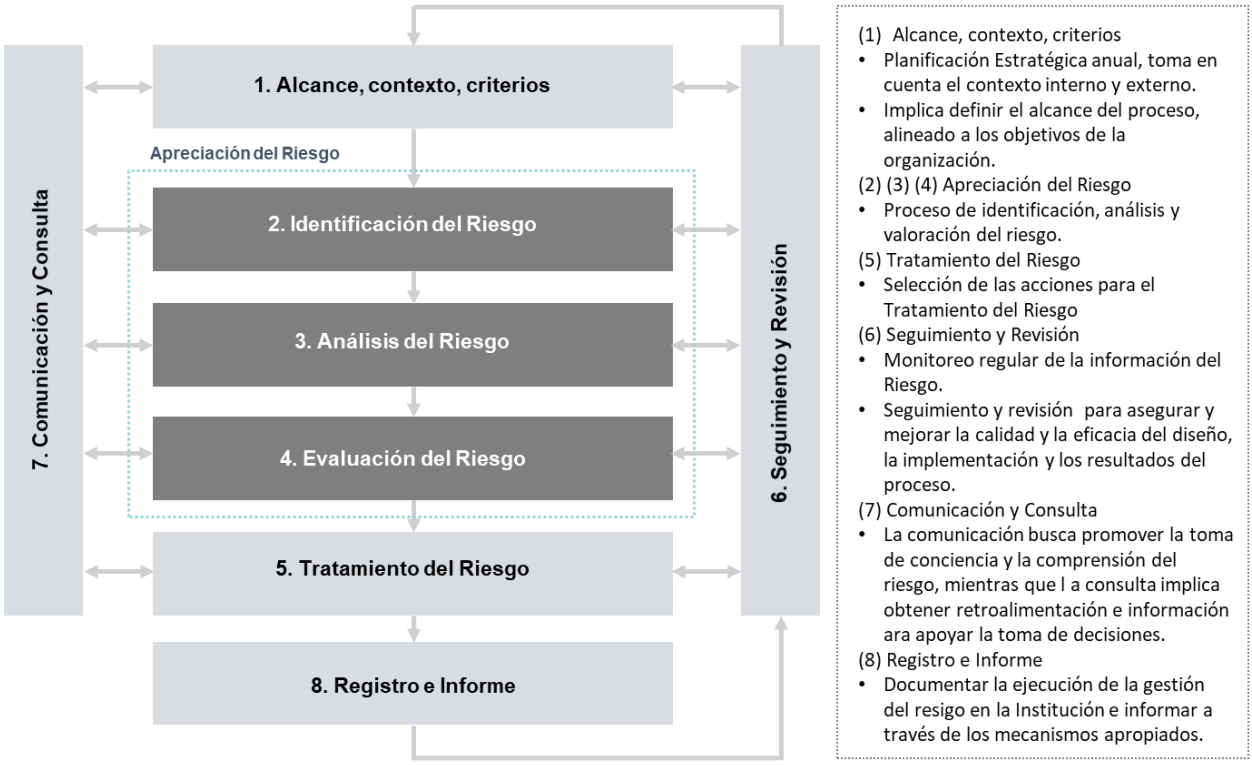

Figura 2: Proceso de Gestión de Riesgos

El proceso puede agruparse en dos fases:

Fase 1 – Alcance, contexto y criterios de Riesgos

- Definición del Alcance, contexto
- Definición/Revisión/Validación de umbrales de impacto y probabilidad
- Factores para la Identificación de Riesgos

Fase 2 – Apreciación y Tratamiento del Riesgo

- Identificación del riesgo.
- Análisis del riesgo.
- Evaluación del riesgo.
- Tratamiento del riesgo.

Fase 1

1. Alcance, contexto y criterios de Riesgos

Abocado a las definiciones generales del contexto y los umbrales, tipos de impactos y criterios de riegos por ámbito de acción, que permitan la identificación de los riesgos en la institución.

a. Definición del Alcance, contexto

Establecer el contexto significa mirar el panorama general y las condiciones actuales o el entorno (interno y externo) que puede afectar los objetivos de **BNF**. Hacer esto ayuda a identificar los riesgos para estos objetivos.

Las funciones de las Divisiones y Unidades de Negocio lo hacen a través del desarrollo de objetivos en cada nivel, así como a través del proceso de planificación estratégica anual. Como el proceso de gestión puede aplicarse a niveles distintos (estratégico, operacional, de programa, de proyecto u otras actividades), es importante definir claramente el alcance considerado.

b. Definición/Revisión/Validación de umbrales de impacto y probabilidad

Los criterios para valorar la importancia del riesgo y apoyar los procesos de toma de decisiones han sido establecidos en una matriz de riesgo como se muestra en la Tabla 1 y Tabla 2, que utilizan 5 rangos definidos de impactos (de muy leve a muy alto) y 5 rangos definidos de probabilidad (de muy baja a muy alta probabilidad).

La gestión del riesgo se ha de realizar por ámbito de gestión[5], por lo que cada uno puede contar con una categoría de impacto única o por ámbito de gestión (esta decisión corresponde al Directorio, puede formalizarse en manuales y/o metodologías independientes):

Valoración		Persona	Operacional	Seguridad -Infraestructura	Ambiental y Social	Reputacional	Legal	TI
1	Muy leve	Accidente menor. Primeros auxilios	Definición en Metodología de Gestión de Riesgo Operacional	No hay ningún impacto en las instalaciones Edilicias. No impide el acceso ni la posibilidad de trabajar.	Definición en Manual de Prácticas, Políticas y Procedimientos de Gestión de Riesgos Ambientales y Sociales, e implementación de un Sistema de Análisis de Riesgos Ambientales y Sociales (SARAS)	Definición en Metodología de Gestión de Riesgo Reputacional	Desafío legal. Acuerdo extrajudicial de menor	Incidente de TI que afecta a un solo servicio / sitio de TI y / o unidad de negocio, pérdida de cobertura en la prestación de los servicios ≤ 1 %
2	Leve	Incidente que requiere tratamiento médico. Menos de 3 días de baja		Se han producido daños estructurales en ciertos sectores del Edificio, no importantes, y se puede acceder a ciertos sectores del mismo.			Acción civil - sin defensa. Aviso de mejora	Incidente de TI que afecta a servicios de TI críticos y / o unidades de negocio, pérdida de cobertura en la prestación de los servicios ≤ 5 %, sin que se haya identificado ninguna solución durante más de 48 horas
3	Medio	Más de 3 días de Reposo. Ingreso en Hospital.		En capacidad de operar por un período corto: pérdida parcial de un sitio o pérdida total de un sitio menor.			Acción colectiva. Enjuiciamiento criminal. Aviso de prohibición	Incidentes de TI que afecten a servicios de TI críticos y / o unidades de negocio, pérdida de cobertura en la prestación de los servicios ≥10 %, sin que se haya identificado ninguna solución durante más de 72 horas. El impacto pone en riesgo la continuidad del negocio
	Alto	Accidente fatal. Inhabilitación permanente		El defecto de infraestructura / activos tiene un impacto moderado en la continuidad del negocio. Cierto nivel de interrupción del negocio e incapacidad para operar			Enjuiciamiento criminal - sin defensa. Ejecutivo despedido	Incidente importante en el Centro de Datos, que afecta a servicios de TI críticos y / o unidades de negocio. Plazos de recuperación inciertos. Pérdida de cobertura en la prestación de los servicios ≥ 20 %.
5	Muy Alto	Fatalidades múltiples. Múltiples inhabilitaciones permanentes		Impacto en el Edificio lo deja fuera de servicio. Se detectan daños estructurales muy importantes y no será posible acceder al mismo en ningún caso			Enjuiciamiento criminal - sin defensa. Ejecutivo multado o encarcelado	Interrupción importante del centro de datos, que requiere la activación de planes de BC / DR para servicios de TI recuperables.

Tabla 1: Umbrales de Impacto

[5] (ISO 9001,14000,45000, MECIP, categorías de riesgos con normativas específicas del ente regulador, etc.)

Dependiendo del ámbito de gestión es posible disponer de diferentes umbrales para la probabilidad de la amenaza:

Probabilidad			
Valoración		Frecuencia	Descripción
5	Muy Alta	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	1vez 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: Umbrales de Probabilidad

c. Definición/Revisión/Validación del criterio del riesgo

El criterio del riesgo es el punto en la escala de valor de riesgo (1 a 25) o calificación del riesgo residual (Muy Bajo a Muy Alto) a partir del cual la Institución considera el riesgo inaceptable.

Los valores de riesgo por encima del criterio se consideran a tratar y los valores por debajo del criterio se consideran aceptables.

En el proceso de evaluación del riesgo que implica el criterio, también se pueden utilizar las opciones transferir o eliminar.

Dado que la escala del riesgo es del 1 al 25 (ver Figura 3) o la calificación del riesgo residual puede resultar en Muy Bajo a Muy Alto (ver Figura 4), tanto el Nivel de Riesgo como el Criterio han de tomar alguno de los siguientes valores:

Probabilidad

Muy Alta	5	5	10	15	20	25
Alta	4	4	8	12	16	20
Media	3	3	6	9	12	15
Baja	2	2	2	6	8	10
Muy Baja	1	1	2	3	4	5
		1	2	3	4	5
		Muy Leve	Leve	Medio	Alto	Muy Alto

Impacto

Figura 3: Matriz de Riesgo

Muy Bajo
Bajo
Medio
Alto
Muy Alto

Figura 4: Calificación del Riesgo

El Directorio tiene la responsabilidad de definir el criterio sobre el que valorar el nivel de riesgo de cada amenaza o riesgo, este criterio se encuentra definido por ámbito de gestión.

Fase 2 – Apreciación y Tratamiento del Riesgo

2. Identificación del Riesgo

Una vez identificados los procesos de negocio, cada uno de los responsables (Propietario del Riesgo) ha de identificar los riesgos por proceso en función de los datos existentes, datos históricos, de su experiencia, de la retroalimentación transmitida por las partes interesadas y de su propio juicio y observación. Esta identificación se debe actualizar en cada ejercicio de apreciación de riesgo.

El propósito de esta identificación de riesgos es encontrar o reconocer, en forma anticipada y continua, los riesgos que tendrán impacto negativo en la capacidad del **BNF** para alcanzar sus objetivos. Toda información ya sea relevante, apropiada y actualizada es importante para identificar riesgos.

El propietario del riesgo puede utilizar una variedad de técnicas para identificar incertidumbres que pueden afectar uno o más de sus objetivos. Los siguientes factores, y las relaciones entre estos factores, deben ser considerados:

- amenazas y oportunidades;
- fuentes de riesgo tangibles e intangibles;
- causas y eventos;
- vulnerabilidades y capacidades,
- capacidad de pago del deudor y comportamiento observado en el cumplimiento de sus obligaciones
- cambios en el contexto externo e interno;
- indicadores de riesgos emergentes;
- identificación de activos;

- la naturaleza y valor de los activos y recursos; mediciones de riesgos (VAR paramétrico, EWMA)
- consecuencias y su impacto en los objetivos;
- limitaciones de conocimiento y confiabilidad de la información;
- factores relacionados con el tiempo,
- Preocupaciones, experiencias, supuestos y creencias de los factores involucrados en la evaluación del riesgo.

El **BNF** al identificar los riesgos debe considerar que puede haber más de un tipo de resultado, lo que puede resultar en una variedad de consecuencias tangibles o intangibles.

3. Análisis del Riesgo

Esta etapa utiliza el resultado de la Identificación de Riesgos para definir los niveles de riesgo. En la mayoría de los ámbitos de gestión, para valorar efectivamente un riesgo, deberá utilizar la matriz de riesgo, la cual examina los niveles de impacto y probabilidad del riesgo identificado, tomando en cuenta la efectividad de los controles implantados.

La valoración final del riesgo deberá reflejar la efectividad de cualquier control y el nivel global de riesgo.

En otros ámbitos de gestión como el de Riesgo de Créditos deberá valorar el riesgo utilizando información del cliente, ratios, indicadores, credit scoring entre otros. El riesgo Financiero deberá valorar mediante mediciones o valoraciones de riesgos y/o modelos estadísticos.

El análisis del riesgo proporcionará las bases para la evaluación del riesgo y para la toma de decisiones relativas al tratamiento del riesgo.

4. Evaluación del Riesgo

La evaluación del riesgo ayuda en la toma de decisiones, basados en los resultados del análisis de riesgos, sobre qué riesgos necesitan tratamiento y la prioridad para la implementación del tratamiento. En la evaluación de riesgo deberá determinar si el nivel de riesgo resultante del análisis es aceptable o no, según el Criterio de Riesgo definido como Apetito y/ Tolerancia al riesgo.

En el caso que los Propietarios del Riesgo propongan la modificación del criterio del Riesgo, deberán solicitar al **Comité de Riesgos**, de manera que este eleve al **Directorio**.

5. Tratamiento del Riesgo

Una vez conocidos los riesgos que exceden el Criterio de Riesgo y se decide tratar, deberá definir los plazos, recursos y responsables de la implementación del tratamiento. Es importante que los tratamientos de riesgo sean identificados, priorizados e implementados vía acciones de Tratamiento por tipos de riesgos.

Se consideran los siguientes tratamientos de riesgo:

- **Evitar** el riesgo, decidiendo no empezar o continuar con la actividad.
- **Tomar** o **incrementar** el riesgo para perseguir una oportunidad.
- **Reducir** el riesgo modificando la probabilidad del riesgo o el impacto del riesgo.
- **Trasferir** el riesgo con otros (incluyendo contratos con aseguradoras).
- **Aceptar** el riesgo con decisión informada.

El tratamiento del riesgo deberá seguir un proceso cíclico de:

- Formulación y selección de la/s opciones/acciones de tratamiento del riesgo en las instancias establecidas para cada categoría (tipo) de riesgo.
- Asignación del responsable/s de la implementación del tratamiento del riesgo.
- Planificación e implementación del tratamiento del riesgo.
- Apreciar la eficacia de ese tratamiento.
- Evaluar si el riesgo luego del tratamiento es aceptable.
- Si no es aceptable, llevar a cabo un tratamiento ulterior.

6. Seguimiento y Revisión

El monitoreo regular de la información en toda la organización asegura que se identifique cualquier indicio de que se esté materializando un riesgo (o que se presente un nuevo riesgo). Esto ayuda a impulsar la toma de decisiones informada. Específicamente, la siguiente información sobre el riesgo se debe monitorear de manera continua:

- Indicadores clave de riesgo: monitoreados y reportados mensualmente.
- Resultados de las auditorías internas (por ejemplo, cualquier cambio identificado en la efectividad del control).
- Riesgos y escaladas identificadas por el negocio (riesgos significativos de las unidades de negocio).

El seguimiento de esta información de riesgo proporciona una indicación de qué medidas tomar. Específicamente, si:

1. Se debe iniciar una evaluación de riesgos a nivel de unidad de negocio o proceso.
2. Se requieren informes adicionales sobre un proyecto, programa o iniciativa específico.
3. Se debe ajustar un plan de tratamiento existente.
4. Se requiere un seguimiento más frecuente.

A su vez, la metodología definida en el presente documento debe mantener un seguimiento periódico a través de las revisiones y actualizaciones pertinentes por parte del Comité de Riesgos, que elevará dichas actualizaciones a aprobación por el Directorio:

- Fase 1 se debe revisar de forma bianual.
- Fase 2 debe realizarse de forma anual.

7. Comunicación y Consulta

La comunicación busca promover la toma de conciencia y la comprensión del riesgo, mientras que la consulta implica obtener retroalimentación e información para respaldar la toma de decisiones.

La estrecha coordinación entre los dos debe facilitar el intercambio de información objetiva, oportuna, relevante, precisa y comprensible, teniendo en cuenta la confidencialidad e integridad de la información, así como los derechos de privacidad de las personas.

La comunicación y la consulta con las partes interesadas externas e internas apropiadas deben tener lugar dentro y durante todos los pasos del proceso de gestión de riesgos. Se debe consultar a las partes interesadas internas y externas durante todo el proceso y se debe comunicar cualquier información relevante (propietarios de riesgos, propietarios de tratamientos) según corresponda.

La consulta y comunicación de riesgos se realiza a través de múltiples vías:

1. Informes de riesgos regulares y continuos incluidas evaluaciones de riesgos de la unidad de negocio.
2. Seguimiento y reporte de planes de tratamiento de riesgos.
3. Capacitación y educación formal sobre gestión de riesgos en toda la organización.
4. Capacitación informal y sensibilización por parte del área de riesgos y los Gestores de Riesgo de la Unidad de Negocio.

La consulta ayuda a establecer el contexto y puede ayudar en la gestión de las partes interesadas, garantizar la participación adecuada de los expertos y generar consenso sobre las actividades futuras de gestión de riesgos. La comunicación de riesgos facilita una mayor transparencia y generalmente conduce a una mejor toma de decisiones.

La Gerencia Departamental de Gestión de Riesgo Integral debe apoyar en el desarrollo del Plan de Comunicación y Concienciación del Riesgo, someter a validación del Gerente de Área de Riesgos quien elevará al Comité de Riesgos para su aprobación final.

Una vez aprobado el Plan de Comunicación y Concienciación, la Gerencia Departamental de Gestión de Riesgo Integral supervisará su ejecución.

8. Registro e Informe

El proceso de gestión de riesgos y sus resultados deberán ser documentados y reportados a través de mecanismos apropiados, por cada área encargada de la gestión de cada categoría o tipo de riesgo.

El registro y la presentación de informes apuntan a:

- Comunicar los resultados y las actividades de gestión de riesgos en toda la organización.
- Proporcionar información para la toma de decisiones;
- Mejorar las actividades de gestión de riesgos;
- Ayudar a la interacción con las partes interesadas, incluidos aquellos con la responsabilidad y la rendición de cuentas para las actividades de gestión de riesgo.

Los registros deberán ser protegidos, permanecer legibles, fácilmente identificables y accesibles, por cada área encargada de la gestión de cada categoría o tipo de riesgo.

El Gerente de Área de Riesgos elabora y remite informes sobre la implementación de la Gestión de Riesgos al Comité de Riesgos y al Directorio.

La Auditoría Interna debe informar los resultados de las evaluaciones sobre la efectividad y el cumplimiento de las etapas de la Gestión Riesgos, informes que debe presentar al Consejo Directivo y al Directorio.

XI. ANEXOS

- Anexo 1: ESTRATEGIA DE GESTION DE RIESGOS
- Anexo 2: DECLARACIÓN DEL APETITO DE RIESGOS